وزارت ارتباطات و فناوری اطلاعات
پژوهشگاه ارتباطات و فناوری اطلاعات

بررسی چارچوب‌های هوش تهدید سایبری

عنوان گزارش: بررسی چارچوب‌های هوش تهدید سایبری

کلمات کلیدی: امنیت سایبری، هوش تهدید سایبری، زنجیره کشتار سایبری، Lockheed Martin، Mitre ATT&CK

تهیه کننده: فاطمه ایمانی مهر

ناظر علمی: مرجان بحرالعلوم

گروه پژوهشی: فناوری امنیت شبکه

سال انتشار: ۱۴۰۳

خلاصه مدیریتی

در دنیای امروز، تهدیدات سایبری به یک چالش اساسی برای سازمان‌ها و دولت‌ها تبدیل شده‌اند. این تهدیدات نه‌تنها می‌توانند باعث خسارات مالی شوند، بلکه اعتبار سازمان‌ها و امنیت اطلاعات کاربران را نیز به خطر می‌اندازند. با افزایش گستره و پیچیدگی این حملات، دیگر نمی‌توان به دفاع‌های سنتی سایبری معمول اکتفا نمود. سازمان‌ها به ابزارها و فرآیندهایی نیاز دارند که به‌صورت پیشگیرانه و در لحظه، بتوانند تهدیدات را شناسایی و ارزیابی کنند. در این میان هوش تهدید سایبری به‌عنوان یک راهکار مؤثر و مهم مطرح گردیده است.

هوش تهدید سایبری به اطلاعات و تحلیل‌هایی اشاره می‌کند که منجر به درک بهتر تهدیدات و حملات سایبری، روش‌های حمله، و اهداف احتمالی مهاجمان می‌گردد. با تجزیه و تحلیل داده‌ها و اطلاعات مختلف از قبیل الگوهای رفتار مهاجم، شناسایی نقاط ضعف و آسیب‌پذیری‌ها، سازمان‌ها می‌توانند دید جامعی از فضای تهدیدات به‌دست آورند. این دید به آن‌ها کمک می‌کند تا از وقوع حملات جلوگیری نموده و یا در صورت وقوع، به‌طور هوشمندانه و به سرعت واکنش نشان دهند.

چارچوب‌های هوش تهدید ساختارهایی را برای فکرکردن در مورد حملات و مهاجمان ارائه می‌دهند. این چارچوب‌ها درک گسترده‌ای از چگونگی فکرکردن مهاجمان، روش‌های مورداستفاده توسط آن‌ها و جایی که در چرخه حیات حمله رویدادهای خاص اتفاق می‌افتد را به‌وجود می‌آورند. این دانش به مدافعان سایبری اجازه می‌دهد که سریع‌تر به حملات واکنش داده و بتوانند آنها را زودتر متوقف کنند. زنجیره کشتار سایبری Lockheed Martin و چارچوب MITRE ATT&CK که از مهمترین چارچوب‌های هوش تهدید هستند، در این گزارش مورد بررسی قرار خواهند گرفت.

زنجیره کشتار سایبری توسط شرکت Lockheed Martin معرفی شده است و با تجزیه و تحلیل مراحل مختلف حمله، به سازمان‌ها کمک می‌کند تا فرآیند حملات را در مراحل ابتدایی شناسایی کرده و از پیشروی آن جلوگیری کنند. این مدل به شناسایی و تجزیه و تحلیل مرحله به مرحلهٔ حملات می‌پردازد و به سازمان‌ها این امکان را می‌دهد که نقاط مختلف حمله را شناسایی کنند و راهکارهایی برای متوقف‌سازی حمله پیاده‌سازی کنند. با تحلیل و شناسایی زودهنگام مراحل اولیه حمله، سازمان‌ها می‌توانند اقدامات پیشگیرانه را قبل از رسیدن به مراحل خطرناک‌تر اجرا کنند.

چارچوب MITRE ATT&CK یک پایگاه دانش مبتنی بر سناریوهای واقعی از حملات سایبری است. این چارچوب توسط موسسه MITRE توسعه داده شده و مجموعه‌ای از تاکتیک‌ها، تکنیک‌ها و رویه‌های (TTP) مورد استفاده مهاجمان را در اختیار سازمان‌ها قرار می‌دهد. MITRE ATT&CK این امکان را فراهم می‌کند که سازمان‌ها نه‌تنها رفتار مهاجمان را بهتر بشناسند، بلکه بتوانند متناسب با تکنیک‌های مورد استفاده آن‌ها، راهکارهای مقابله‌ای خود را بهینه‌سازی کنند. با استفاده از این چارچوب، سازمان‌ها می‌توانند از تاکتیک‌های دفاعی خود یک نقشه جامع ایجاد کرده و رفتارهای مهاجمین را به‌طور دقیق‌تر پیش‌بینی کنند.

در این گزارش، مفاهیم کلی هوش تهدید سایبری بیان گردیده و دو چارچوب مهم یعنی زنجیره کشتار سایبری و MITRE ATT&CK مورد بررسی قرار گرفته است. با توجه به مرجع بودن پایگاه دانش MITRE ATT&CK، بررسی بیشتری روی آن صورت گرفته و علاوه بر معرفی جزئیات ارائه شده در این پایگاه دانش، در مورد نگاشت Enisa Threat Landscape، نگاشت حملات و APTهای مهم به TTPهای Mitre، و استفاده از Mitre برای هوش تهدید نیز مطالبی مهمی بیان گردیده است.

استفاده از این چارچوب‌ها جهت بالا بردن توانمندی دفاع سایبری برای سازمان‌ها بسیار ضروری است. با توجه به اینکه چارچوب Mitre ATT&CK مدام در حال بروزرسانی بر اساس تهدیدات جدیدتر و بروزتر و به تبع آن راه‌های مقابله جدیدتر است، استفاده مستمر از آن نقش بسیار مهمی در به‌روزرسانی دانش تیم امنیتی در زمینه تکنیک‌ها و تاکتیک‌های جدید مهاجمان و راه‌های مقابله با آنها دارد.

بهره‌برداری از هوش تهدید در افزایش تاب‌آوری سایبری سازمان‌ها مؤثر بوده و می‌تواند آمادگی آنها را در برابر تهدیدات نوظهور افزایش دهد. استفاده از چارچوب‌های استاندارد، جهت بالا بردن کارایی اشتراک‌گذاری اطلاعات تهدیدات بین سازمان‌ها، به ویژه از طریق مراکز اشتراک‌گذاری اطلاعات مانند ISACها ضروری است. این امر به تحلیل دقیق‌تر تهدیدات و تقویت دفاع جمعی در کشور تاثیر بسزایی دارد.

فهرست مطالب

۱ مقدمه

در دنیای دیجیتالی و در حال تحول امروزی، تهدیدات سایبری به یک چالش اساسی برای سازمان‌ها و دولت‌ها تبدیل شده‌اند. این تهدیدات نه‌تنها می‌توانند باعث خسارات مالی شوند، بلکه اعتبار سازمان‌ها و امنیت اطلاعات کاربران را نیز به خطر می‌اندازند. با افزایش گستره و پیچیدگی این حملات، دیگر نمی‌توان به دفاع‌های سنتی سایبری معمول اکتفا نمود. سازمان‌ها به ابزارها و فرآیندهایی نیاز دارند که به‌صورت پیشگیرانه و در لحظه، بتوانند تهدیدات را شناسایی و ارزیابی کنند. در این میان هوش تهدید سایبری[۱] به‌عنوان یک راهکار مؤثر و مهم مطرح گردیده است.

هوش تهدید سایبری به اطلاعات و تحلیل‌هایی اشاره می‌کند که منجر به درک بهتر تهدیدات و حملات سایبری، روش‌های حمله، و اهداف احتمالی مهاجمان می‌گردد. با تجزیه و تحلیل داده‌ها و اطلاعات مختلف از قبیل الگوهای رفتار مهاجم، شناسایی نقاط ضعف و آسیب‌پذیری‌ها، سازمان‌ها می‌توانند دید جامعی از فضای تهدیدات داشته باشند. این دید به آن‌ها کمک می‌کند تا از وقوع حملات جلوگیری نموده و یا در صورت وقوع، به‌طور هوشمندانه و به سرعت واکنش نشان دهند. اهمیت این دانش نه‌تنها در شناسایی و مقابله با تهدیدات موجود کمک کننده باشد، بلکه می‌تواند سازمان‌ها را برای مقابله با تهدیدات آینده نیز آماده کند.

چارچوب‌های هوش تهدید ساختارهایی را برای فکرکردن در مورد حملات و مهاجمان ارائه می‌دهند. آن‌ها درک گسترده‌ای از چگونگی فکرکردن مهاجمان، روش‌های مورداستفاده توسط آن‌ها و جایی که در چرخه حیات حمله رویدادهای خاص اتفاق می‌افتد را به‌وجود می‌آورند. این دانش به مدافعان سایبری اجازه می‌دهد که سریع‌تر به حملات واکنش داده و بتوانند آنها را زودتر متوقف کنند. زنجیره کشتار سایبری[۲] Lockheed Martin و چارچوب MITRE ATT&CK از مهمترین مدل‌های هوش تهدید هستند که در این گزارش مورد بررسی قرار خواهند گرفت.

زنجیره کشتار سایبری توسط شرکت Lockheed Martin معرفی شده است و با تجزیه و تحلیل مراحل مختلف حمله، به سازمان‌ها کمک می‌کند تا فرآیند حملات را در مراحل ابتدایی شناسایی کرده و از پیشروی آن جلوگیری کنند. این مدل به شناسایی و تجزیه و تحلیل مرحله به مرحلهٔ حملات می‌پردازد و به سازمان‌ها این امکان را می‌دهد که نقاط مختلف حمله را شناسایی کنند و راهکارهایی برای متوقف‌سازی حمله پیاده‌سازی کنند. با تحلیل و شناسایی زودهنگام مراحل اولیه حمله، سازمان‌ها می‌توانند اقدامات پیشگیرانه را قبل از رسیدن به مراحل خطرناک‌تر اجرا کنند.

چارچوب MITRE ATT&CK یک پایگاه دانش مبتنی بر سناریوهای واقعی از حملات سایبری است. این چارچوب توسط موسسه MITRE توسعه داده شده و مجموعه‌ای از تاکتیک‌ها، تکنیک‌ها و رویه‌های (TTP[۳]) مورد استفاده مهاجمان را در اختیار سازمان‌ها قرار می‌دهد. MITRE ATT&CK این امکان را فراهم می‌کند که سازمان‌ها نه‌تنها رفتار مهاجمان را بهتر بشناسند، بلکه

---

[۱] Cyber Threat Intelligence

[۲] Cyber Kill Chain

[۳] Tactic, Technique, and Procedure

بتوانند متناسب با تکنیک‌های مورد استفاده آن‌ها، راهکارهای مقابله‌ای خود را بهینه‌سازی کنند. با استفاده از این چارچوب، سازمان‌ها می‌توانند از تاکتیک‌های دفاعی خود یک نقشه جامع ایجاد کرده و رفتارهای مهاجمین را به‌طور دقیق‌تر پیش‌بینی کنند.

هدف این گزارش، ارائه یک دیدگاه کلی از هوش تهدید سایبری و بررسی دو چارچوب مهم یعنی زنجیره کشتار سایبری و MITRE ATT&CK است. در این راستا، ابتدا مفاهیم کلی مرتبط با هوش تهدید سایبری بیان گردیده، و سپس با جزئیات بیشتر، دو چارچوب مذکور مورد بررسی قرار می‌گیرند.

۲ هوش تهدید

۲-۱ مقدمه

امروزه فناوری‌های دیجیتال در قلب تقریباً هر صنعتی قرار دارند. هرچند خودکارسازی و اتصالات بیشتر جهان را متحول کرده است ولی آسیب‌پذیری‌های بیشتر در برابر حملات سایبری را نیز به ارمغان آورده است. هوش تهدید دانشی است که امکان پیشگیری از حملات سایبری و کاهش اثر آن‌ها را فراهم می‌کند. هوش تهدید زمینه‌هایی مانند اینکه مهاجمان چه کسانی هستند؟ انگیزه‌ها و قابلیت‌های آن‌ها چیست و چه شاخص‌های مخاطره‌ای (IOC[۱]) در سیستم‌ها باید جستجو شود را فراهم می‌کند. این امر در اتخاذ تصمیمات آگاهانه در مورد امنیت سایبری سازمان‌ها تاثیرگذار است.

امروزه هوش تهدید یک نیاز اصلی برای همه سازمان‌ها است و ارزشی را به عملکردهای امنیتی هر سازمانی با هر اندازه‌ای می‌افزاید. به عنوان مثال:

- **تیم‌های عملیات امنیتی** به‌طور معمول قادر به پردازش جریان عظیم هشدارهایی که دریافت می‌کنند نیستند. **هوش تهدید** را می‌توان با راه‌حل‌های امنیتی که در حال حاضر استفاده می‌کنند ادغام کرد. این به آن‌ها کمک می‌کند تا هشدارها و سایر تهدیدها را به‌طور خودکار اولویت‌بندی و فیلتر کنند.
- **تیم‌های مدیریت آسیب‌پذیری** باید به‌طور دقیق مهم‌ترین آسیب‌پذیری‌ها را اولویت‌بندی کنند. **هوش تهدید** دسترسی به بینش‌ها و زمینه‌های خارجی را فراهم می‌کند که به آن‌ها کمک می‌کند تهدیدهای فوری شرکت خود را از تهدیدهای صرفاً بالقوه متمایز کنند.
- **پیشگیری از تقلب، تحلیل ریسک و سایر کارهای امنیتی سطح بالا** برای درک چشم‌انداز تهدید فعلی به چالش کشیده می‌شوند. **هوش تهدید** بینش‌های کلیدی در مورد عوامل تهدید، مقاصد و اهداف آن‌ها و تاکتیک‌ها، تکنیک‌ها و رویه‌های آن‌ها (TTP) را ارائه می‌دهد.

[۱] Indicator of Compromise

۲-۲ مفاهیم داده، اطلاعات و هوش

سه اصطلاح داده، اطلاعات و هوش تفاوت‌هایی با یکدیگر دارند ولی گاهی بدون دقت زیاد استفاده می‌شوند.

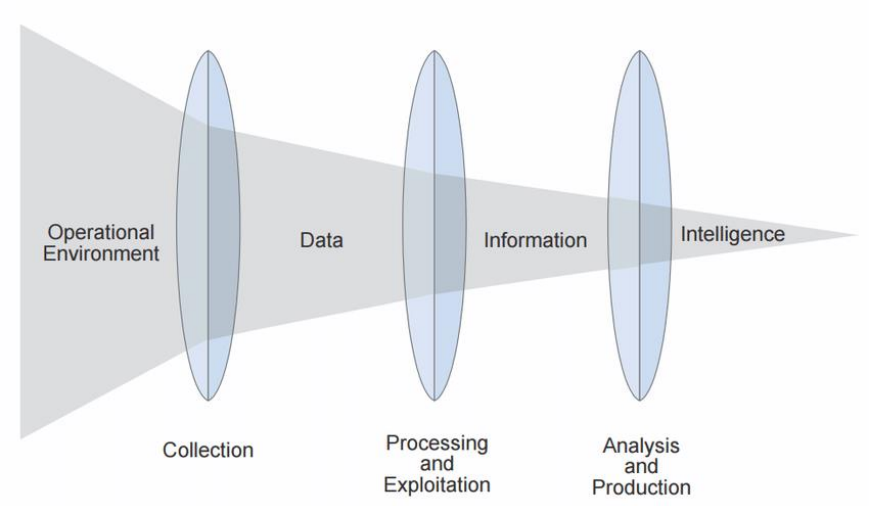
- **داده** شامل حقایق مجزا و آمارهایی است که به‌عنوان مبنایی برای تحلیل بیشتر جمع‌آوری شده است.
- **اطلاعات** چندین داده است که برای پاسخ به سؤالات خاص ترکیب شده‌اند.
- **هوش** داده‌ها و اطلاعات را تحلیل می‌کند تا الگوهایی که به تصمیم‌گیری کمک می‌کنند را آشکار کند.

تعریف داده، اطلاعات و هوش در امنیت سایبری در شکل ۱ آمده است.

داده	داده‌ها معمولاً فقط شاخص‌هایی مانند نشانی IP، URLها یا هش‌ها هستند. داده‌ها بدون تحلیل نمی‌توانند چیز زیادی به ما بگویند.
اطلاعات	اطلاعات به سؤالاتی مانند "این ماه چند بار در رسانه‌های اجتماعی از این سازمان نام برده شده است؟" پاسخ می‌دهند. اگرچه این خروجی بسیار مفیدتر از داده‌های خام است اما هنوز هم به‌طور مستقیم از یک اقدام خاص خبر نمی‌دهد.
هوش	هوش محصول چرخه‌ای از شناسایی سؤالات و اهداف، جمع‌آوری داده‌های مربوطه، پردازش و تحلیل آن‌ها، تولید اطلاعات عملی و توزیع آن اطلاعات است.

شکل ۱ تعریف داده، اطلاعات و هوش در امنیت سایبری

شکل ۲ رابطه بین داده، اطلاعات و هوش در امنیت سایبری را نشان می‌دهد.



شکل ۲ رابطه بین داده، اطلاعات و هوش در امنیت سایبری

۲-۳ تعریف هوش تهدید

هوش تهدید سایبری زیرمجموعه‌ای از هوش است که بر امنیت اطلاعات تمرکز دارد و هدف از آن کمک به سازمان‌ها برای تصمیم‌گیری بهتر در مورد نحوه دفاع از سازمان و کسب‌وکار در برابر تهدیدات سایبری است. برخی از سؤالاتی که هوش تهدید می‌تواند به آن‌ها پاسخ دهد عبارتند از:

- مهاجمین چه کسانی هستند و چگونه ممکن است به حمله کنند؟
- چگونه بردارهای حمله بر امنیت سازمان تأثیر می‌گذارند؟
- تیم‌های عملیات امنیت سازمان باید مراقب چه چیزی باشند؟
- چگونه می‌توان خطر حمله سایبری علیه سازمان را کاهش داد؟

مطابق با تعریف گارتنر[۱] هوش تهدید دانشی است مبتنی بر شواهد (شواهدی از قبیل زمینه، مکانیزم، شاخص‌ها، پیامدها و توصیه‌های عملی) درباره یک تهدید یا خطر موجود یا در حال ظهور برای دارایی‌ها، که می‌تواند برای اطلاع‌رسانی تصمیم‌گیری در مورد واکنش به آن تهدید یا خطر استفاده شود. این مفهوم هوش عملی[۲] است. در واقع به هرگونه هوش که بتواند به اقدامات واقعی منتقل شود و برای راه‌اندازی یک اقدام پیشگیرانه یا تهیه یک استراتژی متقابل استفاده شود هوش عملی گفته می‌شود.

مطابق با تعریف ITU هوش تهدید دانشی است که برای جلوگیری یا کاهش حملات سایبری از جمله انگیزه‌ها، اهداف، ویژگی‌ها، روش‌ها، عملیات، تکنیک‌ها، تاکتیک‌ها و رویه‌های مهاجمان استفاده می‌شود.

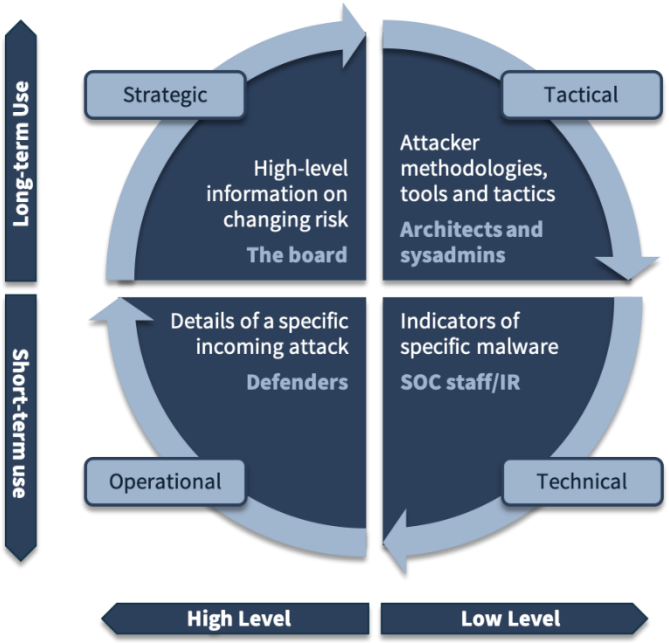
۲-۴ انواع هوش تهدید

هوش تهدید در چهار شکل اصلی وجود دارد: استراتژیک (راهبردی)، تاکتیکی، فنی (تکنیکی) و عملیاتی. دانستن تفاوت‌های بین این چهار نوع می‌تواند در دسته‌بندی یافته‌ها و ایجاد دستورالعمل‌هایی برای جمع‌آوری و پردازش داده‌ها کمک کند. شکل ۳ این چهار دسته هوش تهدید را بر اساس سطح بالا یا سطح پایین بودن و بلندمدت یا کوتاه‌مدت بودن نشان می‌دهد. در ادامه به توضیحاتی در مورد این چهار دسته پرداخته می‌شود.

---

[۱] https://www.gartner.com/doc/۲۴۸۷۲۱۶/definition-threat-intelligence

[۲] Actionable Intelligence



شکل ۳ انواع هوش تهدید

۲-۴-۱ هوش تهدید استراتژیک

این نوع از هوش تهدید گسترده و سطح بالا است و به طور کلی از وضعیت امنیتی، نمایه[۱] کلی ریسک و استراتژی امنیتی اطلاع می‌دهد. هوش تهدید استراتژیک همچنین باید شامل روندهای اجتماعی، صنعتی و سیاسی باشد که می‌تواند بر شرکت و رویکرد آن به امنیت سایبری تأثیر بگذارد. این اطلاعات توسط تیم‌های اجرایی، مدیریت و CISO[۲] استفاده می‌شود.

هوش تهدید استراتژیک اطلاعات سطح بالایی است که در سطح هیئت مدیره یا سایر تصمیم‌گیرندگان ارشد سازمان مصرف می‌شود. معمولاً این نوع از هوش فنی نیست و می‌تواند مواردی مانند تأثیر مالی فعالیت سایبری، روند حملات و مناطقی که ممکن است بر تصمیمات تجاری سطح بالا تأثیر بگذارد را پوشش دهد. به‌عنوان مثال می‌توان گزارشی را مثال زد که نشان می‌دهد احتمال اینکه یک دولت خاص شرکت‌های خارجی که رقبای مستقیم در داخل کشور خود دارند را هک می‌کند. از این رو یک هیئت مدیره ممکن است این واقعیت را در هنگام ارزیابی مزایا و خطرات ورود به آن بازار رقابتی در نظر بگیرد. هوش تهدید استراتژیک تقریباً منحصر به گزارشات یا جلسات توجیهی و یا گفتگو است.

---

[۱] Profile

[۲] Chief Information Security Officer

۲-۴-۲ هوش تهدید عملیاتی

جمع‌آوری هوش تهدید عملیاتی زمینه تهدیدات گذشته و تهدیدات احتمالی آینده را مشخص می‌کند. این نوع هوش تهدید از رفتار انسانی، رسانه‌های اجتماعی و رویدادهای دنیای واقعی جمع‌آوری می‌شود. این اطلاعات توسط رؤسای امنیت و واکنش به حوادث مصرف می‌شود.

هوش تهدید عملیاتی اطلاعاتی در مورد حملات قریب‌الوقوع خاص علیه سازمان است و در ابتدا توسط کارکنان امنیتی سطح بالاتر، مانند مدیران امنیتی یا مدیران واکنش به حادثه، مصرف می‌شود. هر سازمانی دوست دارد هوش تهدید عملیاتی داشته باشد، یعنی بداند چه گروه‌هایی قرار است به آن‌ها حمله کنند، چه زمانی و چگونه. اما چنین اطلاعاتی بسیار نادر است. در اکثر موارد، تنها دولت به گروه‌های مهاجم و زیرساخت‌های لازم برای جمع‌آوری این نوع اطلاعات دسترسی خواهد داشت. برای بسیاری تهدیدات دسترسی قانونی به کانال‌های ارتباطی مربوطه برای یک نهاد خصوصی امکان‌پذیر نیست و از این رو، هوش تهدید عملیاتی در بسیاری موارد گزینه‌ای دردسترس نخواهد بود. با این حال، مواردی وجود دارد که در آن هوش تهدید عملیاتی ممکن است در دسترس باشد، مانند زمانی که یک سازمان توسط هکرهای عمومی هدف قرار می‌گیرد. توصیه می‌شود سازمان‌ها بر روی این موارد تمرکز کنند که در آن جزئیات حملات را می‌توان از اطلاعات منبع باز یا دسترسی به انجمن‌های گفتگوی بسته پیدا کرد.

شکل دیگری از هوش تهدید عملیاتی که ممکن است در دسترس باشد از حملات مبتنی بر فعالیت ناشی می‌شود که در آن فعالیت‌ها یا رویدادهای خاص در دنیای واقعی منجر به حملات در حوزه سایبری می‌شود. در چنین مواردی، گاهی اوقات می‌توان حملات آینده را پس از رویدادهای خاص پیش‌بینی کرد. این ارتباط حملات با رویدادهای دنیای واقعی، در امنیت فیزیکی رایج است اما در امنیت سایبری کمتر دیده می‌شود.

۲-۴-۳ هوش تهدید تاکتیکی

هوش تهدید تاکتیکی به بردارهای حمله، قابلیت‌های امنیت سایبری و افشای دانشی که می‌تواند در بروز نقض نقش داشته باشد نگاه می‌کند. این اطلاعات توسط متخصصان امنیت سایبری، معماران و مدیران استفاده می‌شود.

هوش تهدید تاکتیکی اغلب به عنوان تاکتیک‌ها، تکنیک‌ها و رویه‌ها (TTP) شناخته می‌شود و اطلاعاتی در مورد نحوه انجام حملات توسط بازیگران تهدید است. هوش تهدید تاکتیکی توسط مدافعان و واکنش‌دهندگان به حادثه مصرف می‌شود تا اطمینان حاصل شود که دفاع، هشدار و تحقیقات آن‌ها برای تاکتیک‌های فعلی آماده شده است. به‌عنوان مثال، این واقعیت که مهاجمان از ابزارهایی (اغلب مشتقات Mimikatz) برای به‌دست‌آوردن اعتبارنامه و سپس پخش مجدد آن اعتبارنامه‌ها از طریق PsExec استفاده می‌کنند، یک هوش تاکتیکی است که می‌تواند مدافعان را به تغییر خط‌مشی ترغیب کند. هوش تهدید تاکتیکی اغلب با خواندن مقالات، برقراری ارتباط با همتایان در سازمان‌های دیگر برای یادگیری آنچه که مهاجمان انجام می‌دهند یا خرید از ارائه‌دهندگان چنین اطلاعاتی به دست می‌آید.

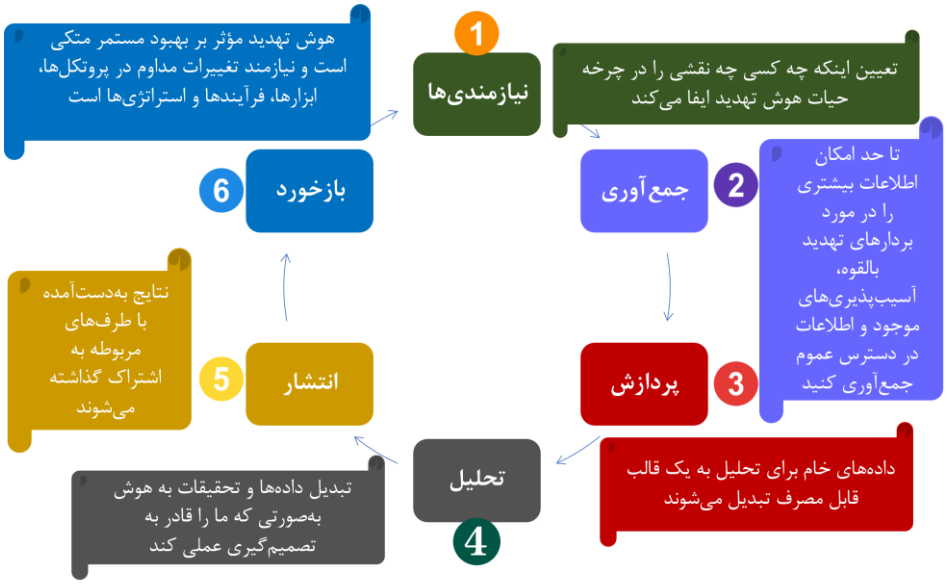
۲-۴-۴ هوش تهدید فنی

هوش تهدید فنی مربوط به شاخص‌هایی از حملات خاصی است که سازمان‌ها می‌توانند به آن توجه کنند، به‌ویژه وقتی صحبت از مهندسی اجتماعی می‌شود. این نوع اطلاعات باید مرتباً به‌روز شوند زیرا حملات سایبری دائماً در حال تغییر هستند.

هوش تهدید فنی داده‌ها یا اطلاعاتی است که معمولاً از طریق ابزارهای فنی مصرف می‌شود. یک مثال می‌تواند فیدهای آدرس‌های IP باشد که مشکوک به مخرب‌بودن به‌عنوان سرورهای فرمان و کنترل[۱] هستند. هوش تهدید فنی اغلب عمر کوتاهی دارد زیرا مهاجمان می‌توانند به‌راحتی آن‌ها را تغییر دهند، بنابراین نیاز به مصرف خودکار چنین اطلاعاتی وجود دارد. هوش تهدید فنی معمولاً عملکردهای تحقیقاتی یا نظارتی یک کسب و کار را تغذیه می‌کند، به‌عنوان مثال با مسدودکردن تلاش برای اتصال به سرورهای مشکوک.

۲-۵ چرخه حیات هوش تهدید

هوش تهدید مبتنی بر تکنیک‌های تحلیلی است که طی چندین دهه توسط سازمان‌های دولتی و نظامی تقویت شده است. هوش تهدید بر شش مرحله متمایز تمرکز دارد که «چرخه هوشمندی» را تشکیل داده و چرخه حیات هوش تهدید نامیده می‌شود. این شش مرحله عبارتند از: نیازمندی‌ها، جمع‌آوری، پردازش، تحلیل، انتشار و بازخورد. شکل ۴ خلاصه‌ای از کارهای انجام‌شده در این شش مرحله را نشان می‌دهد. در ادامه توضیحات بیشتری در مورد این مراحل ارائه می‌شود.



شکل ۴ چرخه حیات هوش تهدید

[۱] Command and Control

۲-۵-۱ مرحله نیازمندی‌ها

مرحله نیازمندی‌ها از چرخه حیات هوش تهدید زمانی است که شما اهدافی را برای برنامه هوش تهدید تعیین می‌کنید که شامل درک و بیان موارد زیر است:

- دارایی‌های اطلاعاتی و فرآیندهای تجاری که نیاز به محافظت دارند.
- اثرات بالقوه مربوط به از دست دادن آن دارایی‌ها یا قطع آن فرآیندها.
- انواع هوش تهدید که سازمان امنیتی برای محافظت از دارایی‌ها و پاسخ‌گویی به تهدیدات نوظهور به آن نیاز دارد.
- اولویت‌ها در مورد آنچه باید محافظت شود.

هنگامی‌که نیازهای هوش در سطح بالا مشخص شد، سازمان می‌تواند سؤالاتی را فرموله کند که نیاز به اطلاعات را به نیازمندی‌های گسسته هدایت کند. به‌عنوان مثال، اگر هدف درک مهاجمین احتمالی باشد، یک سوال منطقی این خواهد بود که "کدام عوامل تهدید در انجمن‌های زیرزمینی به طور فعال اطلاعات مربوط به سازمان ما را درخواست می‌کنند؟"

۲-۵-۲ مرحله جمع‌آوری

مرحله جمع‌آوری فرآیند جمع‌آوری اطلاعات برای رسیدگی به مهم‌ترین نیازهای هوش است. جمع‌آوری اطلاعات می‌تواند به صورت ارگانیک از طرق مختلف انجام شود، از جمله:

- بیرون کشیدن متاداده و گزارش‌ها از شبکه‌های داخلی و دستگاه‌های امنیتی
- اشتراک در فیدهای داده تهدید از سازمان‌های صنعتی و فروشندگان امنیت سایبری
- برگزاری گفتگو و مصاحبه هدفمند با منابع آگاه
- اسکن اخبار و وبلاگ‌های منبع باز (یک روش معمول OSINT)
- جستوجو در وب‌سایت‌ها و انجمن‌ها
- نفوذ به منابع بسته مانند انجمن‌های وب تاریک

داده‌های جمع‌آوری‌شده معمولاً ترکیبی از اطلاعات هوش تمام‌شده، مانند گزارش‌های هوش کارشناسان و فروشندگان امنیت سایبری، و داده‌های خام، مانند امضای بدافزار یا اعتبارنامه‌های افشاشده خواهد بود.

۲-۵-۳ مرحله پردازش

پردازش تبدیل اطلاعات جمع‌آوری‌شده به فرمت قابل استفاده توسط سازمان است. تقریباً تمام داده‌های خام جمع‌آوری‌شده باید به شیوه‌ای پردازش شوند، چه توسط انسان یا ماشین. روش‌های مختلف جمع‌آوری اغلب به ابزارهای مختلف پردازش نیاز دارند. گزارش‌های انسانی ممکن است نیاز به همبستگی و رتبه‌بندی، رفع تعارض و بررسی داشته باشند.

یک مثال می‌تواند استخراج آدرس‌های IP از گزارش یک فروشنده امنیتی و افزودن آن‌ها به یک فایل CSV برای استفاده در یک SIEM باشد. در یک حوزه فنی‌تر، پردازش ممکن است شامل استخراج شاخص‌ها از یک ایمیل، غنی‌سازی آن‌ها با اطلاعات دیگر و سپس برقراری ارتباط با ابزارهای حفاظت نقطه پایانی[۱] برای مسدودسازی خودکار باشد.

۲-۵-۴ مرحله تحلیل

تحلیل یک فرآیند انسانی است که اطلاعات پردازش‌شده را به هوش تبدیل می‌کند که می‌تواند تصمیماتی را اتخاذ کند. بسته به شرایط، تصمیمات ممکن است شامل بررسی تهدیدات بالقوه نوظهور، اقدامات فوری برای جلوگیری از حمله، چگونگی تقویت کنترل‌های امنیتی یا میزان سرمایه‌گذاری در منابع امنیتی اضافی باشد. شکلی که اطلاعات در آن ارائه می‌شود از اهمیت ویژه‌ای برخوردار است. به‌عنوان مثال، اگر می‌خواهید با مدیران غیرفنی ارتباط برقرار کنید، گزارش شما باید:

- مختصر باشد (یادداشت یک صفحه‌ای یا تعدادی اسلاید).
- از اصطلاحات گیج‌کننده و بیش از حد فنی خودداری کنید.
- مسائل را در شرایط تجاری بیان کنید (مانند هزینه‌های مستقیم و غیرمستقیم و تأثیر بر شهرت).
- شامل توصیه‌های عملی باشد.

ممکن است لازم باشد برخی از اطلاعات هوش در قالب‌های مختلف برای مخاطبان مختلف ارائه شود، مثلاً با ارائه پاورپوینت و لازم نیست همه اطلاعات از طریق یک گزارش رسمی بیان شوند. تیم‌های هوش تهدیدات سایبری موفق، گزارش‌های فنی مستمری را به سایر تیم‌های امنیتی پیرامون IOC، بدافزارها، عوامل تهدید، آسیب‌پذیری‌ها و روندهای تهدید ارائه می‌کنند.

۲-۵-۵ مرحله انتشار

انتشار شامل رساندن خروجی هوش نهایی به مکان‌هایی است که نیاز است خروجی به دست آن‌ها برسد. بیشتر سازمان‌های امنیت سایبری چند تیم دارند که می‌توانند از هوش تهدید بهره ببرند. برای هر یک از این مخاطبان، باید موارد زیر را بپرسید:

- آن‌ها به چه نوع هوش تهدیدی نیاز دارند؟
- هوش چگونه باید ارائه شود تا برای آن‌ها به‌راحتی قابل درک و عملی باشد؟
- هر چند وقت یک‌بار باید به‌روزرسانی‌ها و سایر اطلاعات به آن‌ها ارائه شود؟
- هوش باید از طریق چه رسانه‌ای منتشر شود؟

---

[۱] Endpoint

۲-۵-۶ مرحله بازخورد

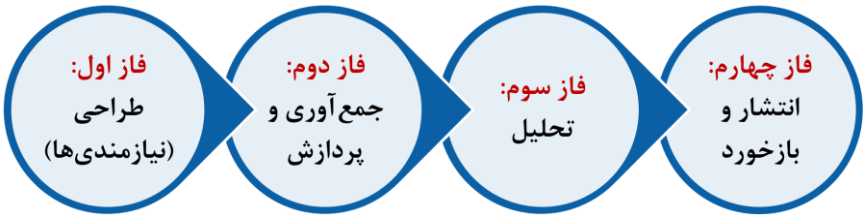
درک اولویت‌های کلی هوش و الزامات تیم‌های امنیتی که هوش تهدید را مصرف می‌کنند بسیار مهم است. نیازهای آن‌ها تمام مراحل چرخه حیات هوش تهدید را هدایت می‌کند و به سازمان می‌گوید که:

- چه نوع داده‌هایی جمع‌آوری شود.
- نحوه پردازش و غنی‌سازی داده‌ها برای تبدیل آن‌ها به اطلاعات مفید را ارائه می‌دهد.
- چگونه اطلاعات را تحلیل کنیم و آن را به‌عنوان هوش تهدید عملی ارائه کنیم.
- هر نوع هوش باید به چه کسی منتشر شود، با چه سرعتی منتشر شود و با چه سرعتی می‌توان به سؤالات پاسخ داد.

سازمان به بازخورد منظم نیاز دارد تا مطمئن شود که الزامات و نیازمندی‌های هر گروه را درک کرده است و با تغییر الزامات و اولویت‌های آن‌ها هماهنگ شود.

۲-۶ ادغام هوش تهدید در عملیات امنیتی

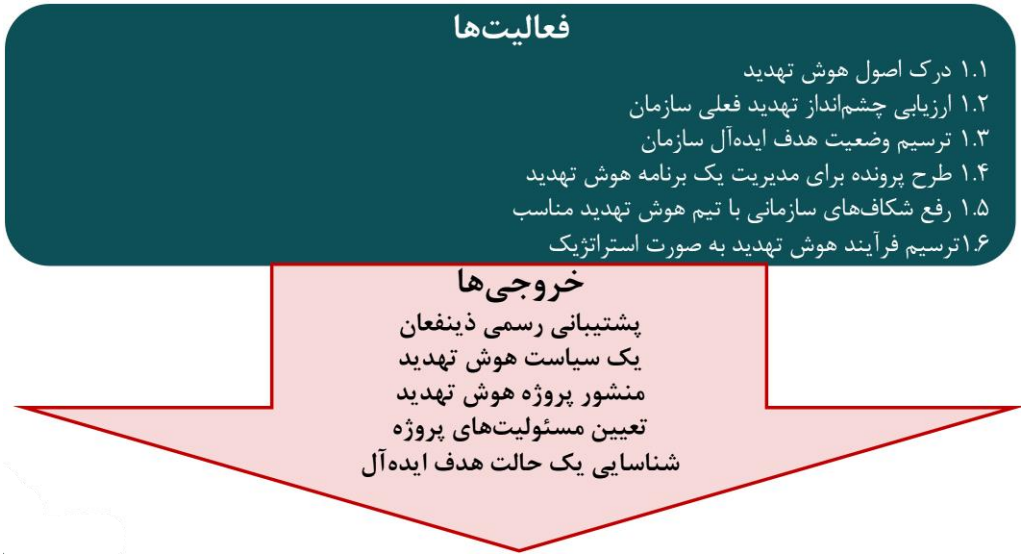
گروه تحقیقاتی infotech اقدام به برگزاری کارگاه با عنوان ادغام هوش تهدید در عملیات امنیتی سازمان کرده است[۱]. در این کارگاه برای ادغام هوش تهدید در عملیات امنیتی چهار فاز نشان داده شده در شکل ۵ پیشنهاد شده است. همان‌طور که در این شکل مشاهده می‌شود، این فازها کاملاً منطبق با چرخه حیات هوش تهدید هستند. به عبارت بهتر، فاز اول منطبق با مرحله اول چرخه حیات هوش تهدید، فاز دوم منطبق با مراحل دوم و سوم چرخه حیات هوش تهدید، فاز سوم منطبق با مرحله چهارم چرخه حیات هوش تهدید و فاز چهارم منطبق با مراحل پنجم و ششم چرخه حیات هوش تهدید می‌باشد.



شکل ۵ ادغام هوش تهدید در عملیات امنیتی

فعالیت‌های تعریف‌شده برای هر فاز و خروجی‌های مورد انتظار برای آن فاز به‌صورت خلاصه در قالب شکل‌های ۶ تا ۹ ارائه شده است.

[۱] https://www.infotech.com/research/ss/integrate-threat-intelligence-into-your-security-operations



شکل ۶ ادغام هوش تهدید در عملیات امنیتی (فعالیت‌ها و خروجی‌های فاز اول)

شکل ۷ ادغام هوش تهدید در عملیات امنیتی (فعالیت‌ها و خروجی‌های فاز دوم)

شکل ۸ ادغام هوش تهدید در عملیات امنیتی (فعالیت‌ها و خروجی‌های فاز سوم)

شکل ۹ ادغام هوش تهدید در عملیات امنیتی (فعالیت‌ها و خروجی‌های فاز چهارم)

۳ چارچوب‌های هوش تهدید

چارچوب‌های هوش تهدید ساختارهایی را برای فکرکردن در مورد حملات و مهاجمان ارائه می‌دهند. آن‌ها درک گسترده‌ای از چگونگی فکرکردن مهاجمان، روش‌های مورداستفاده توسط آن‌ها و جایی که در چرخه حیات حمله رویدادهای خاص اتفاق می‌افتد را به‌وجود می‌آورند. این دانش به مدافعان اجازه می‌دهد که واکنش‌های قاطعانه‌ی سریع‌تر گرفته و حمله را زودتر متوقف کنند. این چارچوب‌ها همچنین به تمرکز بر جزئیاتی که نیاز به بررسی بیشتر دارند تا اطمینان حاصل شود که تهدیدها کاملاً حذف شده‌اند و اقداماتی که برای جلوگیری از نفوذهای مشابه در آینده انجام شده است مناسب هستند. در نهایت، این چارچوب‌ها برای به‌اشتراک‌گذاری اطلاعات در داخل و بین سازمان‌ها مفید هستند. آن‌ها یک دستور زبان و نحو مشترک برای توضیح جزئیات حملات و چگونگی ارتباط آن جزئیات با یکدیگر ارائه می‌دهند. یک چارچوب مشترک، دریافت هوش تهدید از منابعی مانند فروشندگان هوش تهدید، تالارهای گفتمان منبع باز و مراکز به‌اشتراک‌گذاری و تحلیل اطلاعات (ISAC) را آسان‌تر می‌کند. چارچوب‌های هوش تهدید رقابتی نیستند، بلکه مکمل یکدیگرند. می‌توان از چند تا از این چارچوب‌ها با هم استفاده کرد. در ادامه دو چارچوب Lockheed Martin Cyber Kill Chain و MITRE ATT&CK که مهم‌ترین چارچوب‌های هوش تهدید هستند مورد بررسی قرار می‌گیرند.

۳-۱ چارچوب Lockheed Martin Cyber Kill Chain

چارچوب Cyber Kill Chain[۱] برای اولین بار توسط Lockheed Martin در سال ۲۰۱۱ میلادی توسعه داده شد. Cyber Kill Chain از شناخته‌شده‌ترین چارچوب‌های هوش تهدید است که بر اساس مفهوم نظامی زنجیره کشتار عمل می‌کند که در آن ساختار حمله به مراحلی شکسته می‌شود. این چارچوب هفت مرحله را در یک حمله توصیف می‌کند (شکل ۱۰).

۱. شناسایی[۲]
۲. اسلحه‌سازی[۳]
۳. تحویل[۴]
۴. بهره‌برداری[۵]
۵. نصب و راه‌اندازی[۶]

---

[۱] https://www.lockheedmartin.com

[۲] Reconnaissance

[۳] Weaponization

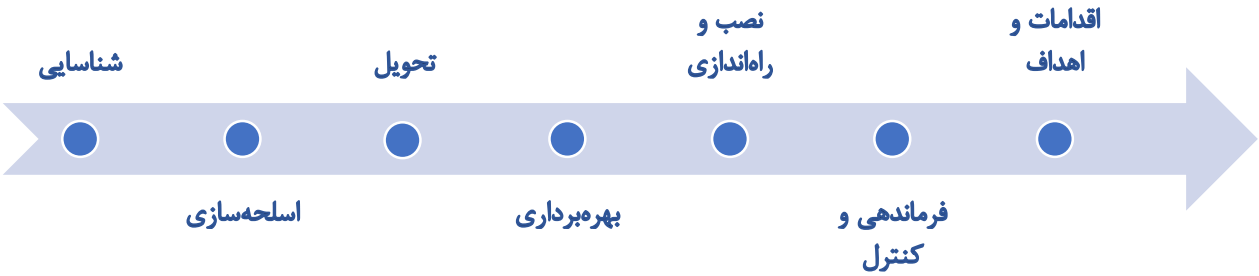
[۴] Delivery

[۵] Exploitation

[۶] Installation

۶. فرماندهی و کنترل[۱]
۷. اقدامات و اهداف[۲]

تیم‌های امنیتی می‌توانند پاسخ‌های استانداردی را برای هر مرحله گسترش دهند. به‌عنوان مثال اگر هدف متوقف‌کردن حمله در مرحله‌ی بهره‌برداری است باید اطمینان بالا داشته باشید که هیچ چیزی بر روی سیستم‌های هدف نصب نشده است. بنابراین ممکن است به فعالیت کامل واکنش به حادثه نیاز نباشد.



شکل ۱۰ مراحل مختلف در چارچوب Cyber Kill Chain

شکل ۱۱ خلاصه‌ای از کارهای انجام‌گرفته در هر مرحله را نشان می‌دهد. این مراحل در ادامه با توضیحات بیشتر توصیف می‌شوند.

[۱] Command and Control

[۲] Actions

شکل ۱۱ خلاصه‌ای از کارهای انجام‌گرفته در مراحل مختلف از چارچوب Cyber Kill Chain

۳-۱-۱ مرحله شناسایی

این مرحله شامل جمع‌آوری اطلاعات در مورد هدف می‌باشد (اطلاعاتی از قبیل برشماری[۱] شبکه، نشانی‌های ایمیل، رسانه اجتماعی و غیره). در ادامه این مرحله را از دید مهاجم[۲] و مدافع[۳] مورد بررسی قرار می‌دهیم.

- **مهاجم**

مهاجمین در مرحله برنامه‌ریزی عملیات خود هستند. آن‌ها تحقیقاتی را انجام می‌دهند تا بفهمند کدام اهداف[۴] آن‌ها را قادر می‌سازد به مقصود خود برسند.

- جمع‌آوری نشانی‌های ایمیل
- شناسایی کارمندان در شبکه های اجتماعی
- جمع‌آوری نشریات مطبوعاتی، جوایز قرارداد و لیست شرکت‌کنندگان کنفرانس
- کشف سرورهای قابل دسترس از طریق اینترنت

[۱] Enumeration
[۲] Attacker
[۳] Defender
[۴] Targets

- **مدافع**

تشخیص شناسایی در صورت وقوع می‌تواند بسیار دشوار باشد، اما کشف شناسایی می‌تواند هدف مهاجمین را آشکار کند.

- جمع‌آوری لاگ‌های مربوط به بازدیدکنندگان وبگاه به‌منظور هشدار و جست‌وجوی تاریخچه
- همکاری با مدیران وب برای استفاده از تحلیل مرورگر موجود
- ساخت تشخیص‌هایی برای رفتارهای مرور منحصربه‌فرد
- اولویت‌بندی دفاع در مورد فناوری‌های خاص یا افراد

۳-۱-۲ مرحله اسلحه‌سازی

این مرحله شامل اضافه‌کردن اکسپلویت به کد مخرب است (مانند سند PDF، تزریق الگو از راه دور و غیره). در ادامه این مرحله را از دید مهاجم و مدافع مورد بررسی قرار می‌دهیم.

- **مهاجم**

مهاجمین در مرحله آماده‌سازی عملیات خود هستند. تولید بدافزار به احتمال زیاد با دست انجام نمی‌شود بلکه از ابزارهای خودکار استفاده می‌شود. یک «سلاح‌ساز[۱]» بدافزار را با اکسپلویت در یک پیلود قابل تحویل جفت می‌کند.

- تهیه یک سلاح‌ساز در داخل یا از طریق کانال‌های عمومی یا خصوصی
- انتخاب سند "decoy" برای ارائه به قربانی (برای اکسپلویت‌های مبتنی بر فایل)
- انتخاب درب پشتی و زیرساخت فرماندهی و کنترل مناسب برای عملیات
- کامپایل درب پشتی و تبدیل پیلود به سلاح

- **مدافع**

این یک مرحله ضروری برای مدافعان است. اگرچه آن‌ها نمی‌توانند سلاح‌سازی را همان‌طور که اتفاق می‌افتد تشخیص دهند ولی می‌توانند با تحلیل مصنوعات بدافزار آن را استنباط کنند.

- انجام تحلیل کامل بدافزار
- ساخت تشخیص‌هایی برای سلاح‌سازها
- تحلیل زمان ایجاد بدافزار نسبت به زمان استفاده از آن
- جمع‌آوری فایل‌ها و متاداده‌ها برای تحلیل آینده
- تعیین اینکه مصنوعات سلاح‌ساز در کدام کمپین‌های APT وجود دارند

[۱] Weaponizer

۳-۱-۳ مرحله تحویل

این مرحله شامل تحویل کد مخرب به قربانی است (به روش‌هایی از قبیل ایمیل، USB، وبگاه مورد مخاطره قرار گرفته و غیره). در ادامه این مرحله را از دید مهاجم و مدافع مورد بررسی قرار می‌دهیم.

- **مهاجم**

در این مرحله مهاجمین بدافزار را به هدف منتقل می‌کنند. آن‌ها عملیات خود را آغاز کرده‌اند.

- ایمیل مخرب
- بدافزار در USB
- تعاملات رسانه‌های اجتماعی
- "Watering hole" در وبگاه‌های مورد مخاطره قرار گرفته

- **مدافع**

این مرحله اولین و مهم‌ترین فرصت برای مدافعان برای جلوگیری از عملیات است. یکی از معیارهای کلیدی اثربخشی، درصدی از تلاش‌های نفوذ است که در مرحله تحویل مسدود می‌شوند.

- تحلیل رسانه تحویل.
- درک سرورها و افراد مورد هدف قرار گرفته، نقش‌ها و مسئولیت‌ها و اطلاعات موجود نزد آن‌ها.
- استنباط قصد مهاجم بر اساس هدف‌گیری.
- استفاده از مصنوعات سلاح‌ساز برای شناسایی پیلودهای مخرب جدید در نقطه تحویل.
- تحلیل زمان شروع عملیات.
- جمع‌آوری ایمیل و لاگ‌های وب برای بازسازی فارنزیک. حتی اگر نفوذ دیر تشخیص داده شود، مدافعان باید بتوانند تعیین کنند که تحویل چه زمانی و چگونه آغاز شده است.

۴-۱-۳ مرحله بهره‌برداری

این مرحله شامل بهره‌برداری از یک قربانی مورد هدف قرار گرفته با استفاده از یک آسیب‌پذیری است. در ادامه این مرحله را از دید مهاجم و مدافع مورد بررسی قرار می‌دهیم.

- **مهاجم**

مهاجمین باید از یک آسیب‌پذیری برای به‌دست‌آوردن دسترسی سوءاستفاده کنند.

- نرم‌افزار، سخت‌افزار یا آسیب‌پذیری انسانی
- توسعه‌دادن بهره‌برداری روز صفر
- ایجاد اکسپلویت‌هایی برای آسیب‌پذیری‌های مبتنی بر سرور
- قربانی اکسپلویت را راه‌اندازی می‌کند

- بازکردن پیوست ایمیل مخرب
- کلیک‌کردن روی پیوند مخرب

- **مدافع**

در این مرحله مدافع اقدامات امن‌سازی انعطاف‌پذیری را اضافه می‌کند.

- آموزش آگاهی کاربر و تست ایمیل برای کارمندان
- آموزش کدنویسی امن برای توسعه‌دهندگان وب
- اسکن منظم آسیب‌پذیری و تست نفوذ
- اقدامات امن‌سازی نقطه پایانی
  - محدودسازی امتیازات مدیریت
  - استفاده از مایکروسافت EMET
  - قوانین نقطه پایانی سفارشی برای مسدودسازی اجرای کد پوسته
- ممیزی پردازه نقطه پایانی برای تعیین منشاء بهره‌برداری از نظر فارنزیک

۳-۱-۵ مرحله نصب و راه‌اندازی

در این مرحله کد مخرب در سیستم از طریق درب‌های پشتی، ابزارهای راه دور و غیره نصب می‌شود. در ادامه این مرحله را از دید مهاجم و مدافع مورد بررسی قرار می‌دهیم.

- **مهاجم**

به طور معمول، مهاجمین یک درب پشتی را در محیط قربانی نصب می‌کنند تا دسترسی را برای مدت طولانی حفظ کنند.

- نصب webshell روی وب سرور
- نصب درب پشتی روی سیستم مشتری
- ایجاد ماندگاری با افزودن سرویس‌ها، کلیدهای AutoRun و غیره

- **مدافع**

استفاده از ابزارها در نقطه پایانی برای شناسایی و ثبت فعالیت نصب. مرحله نصب را در حین تحلیل بدافزار تحلیل کنید تا روش‌های جدید دفاع را ایجاد کنید.

- استفاده از HIPS برای هشدار یا مسدودسازی مسیرهای نصب رایج
- درک اینکه آیا بدافزار به دسترسی مدیر هم نیاز دارد یا فقط به دسترسی کاربر عادی نیاز دارد
- ممیزی نقطه پایانی برای کشف ایجاد فایل‌های غیرعادی
- استخراج گواهی مربوط به هر فایل اجرایی امضاشده
- درک زمان کامپایل بدافزار برای تشخیص قدیمی یا جدید بودن آن

۳-۱-۶ مرحله فرماندهی و کنترل

در این مرحله ارتباط با مهاجم از طریق سیستم اکسپلویت‌شده انجام می‌شود. در ادامه این مرحله را از دید مهاجم و مدافع مورد بررسی قرار می‌دهیم.

- **مهاجم**

بدافزار یک کانال فرمان باز می‌کند تا مهاجم را قادر به دستکاری قربانی از راه دور نماید.

- بازکردن کانال‌های ارتباطی دوطرفه به زیرساخت C۲
- بیشتر کانال‌های رایج C۲ از طریق پروتکل‌های وب، DNS و ایمیل هستند
- زیرساخت C۲ ممکن است متعلق به مهاجم باشد یا اینکه خودش شبکه قربانی دیگری باشد

- **مدافع**

آخرین فرصت مدافع برای جلوگیری از عملیات با مسدودسازی کانال C۲. اگر مهاجمین نتوانند دستورات را ارسال کنند، مدافعان می‌توانند از تأثیر حمله جلوگیری کنند.

- کشف زیرساخت‌های C۲ با تحلیل کامل بدافزار
- سخت‌سازی[۱] شبکه
- سفارشی‌سازی بلاک‌های پروتکل‌های C۲ در پروکسی‌های وب
- DNS Sinkholing و مسمومیت سرور نام[۲]
- انجام تحقیقات منبع باز برای کشف زیرساخت‌های جدید C۲ مهاجم

۳-۱-۷ اقدامات و اهداف

در این مرحله مهاجم به اهداف خود دسترسی پیدا می‌کند (اهدافی از قبیل استخراج داده، به‌دست‌آوردن دسترسی بیشتر به محیط، اخاذی و غیره). در ادامه این مرحله را از دید مهاجم و مدافع مورد بررسی قرار می‌دهیم.

- **مهاجم**

- جمع‌آوری اطلاعات کاربری
- افزایش امتیازات
- شناسایی داخلی

---

[۱] Harden

[۲] Name Server Poisoning

- حرکت جانبی در محیط
- جمع‌آوری و استخراج داده‌ها
- از بین بردن سیستم‌ها
- بازنویسی یا خراب‌کردن داده‌ها
- تغییر مخفیانه داده‌ها

- **مدافع**

هر چه مهاجم برای زمان طولانی‌تر به این مرحله دسترسی داشته باشد تأثیر آن بیشتر است. مدافعان باید این مرحله را در اسرع وقت با استفاده از شواهد فارنزیک از جمله ضبط بسته‌های شبکه، برای ارزیابی شناسایی کنند.

- تنظیم Playbook واکنش به حادثه، از جمله مشارکت اجرایی و طرح ارتباطات
- شناسایی استخراج داده‌ها، حرکت جانبی، استفاده غیرمجاز از اعتبارنامه
- پاسخ فوری تحلیلگر به همه هشدارها
- استقرار عوامل فارنزیک از قبل به نقاط پایانی برای تریاژ سریع
- ضبط بسته شبکه برای ایجاد مجدد فعالیت
- انجام ارزیابی خسارت با کارشناسان موضوع

۲-۳ چارچوب MITRE ATT&CK

چارچوب MITRE ATT&CK[۱] در سال ۲۰۱۳ میلادی ایجاد شد. چارچوب MITRE ATT&CK به عنوان یک پایگاه دانش مدیریت‌شده و مشترک جهانی از تاکتیک‌ها، تکنیک‌ها و رویه‌های متخاصم، یک طبقه‌بندی مشترک از حملات و دفاع‌ها برای مدل‌سازی بهتر تهدید، هوش تهدید سایبری، شبیه‌سازی خصمانه و غیره ارائه می‌دهد.

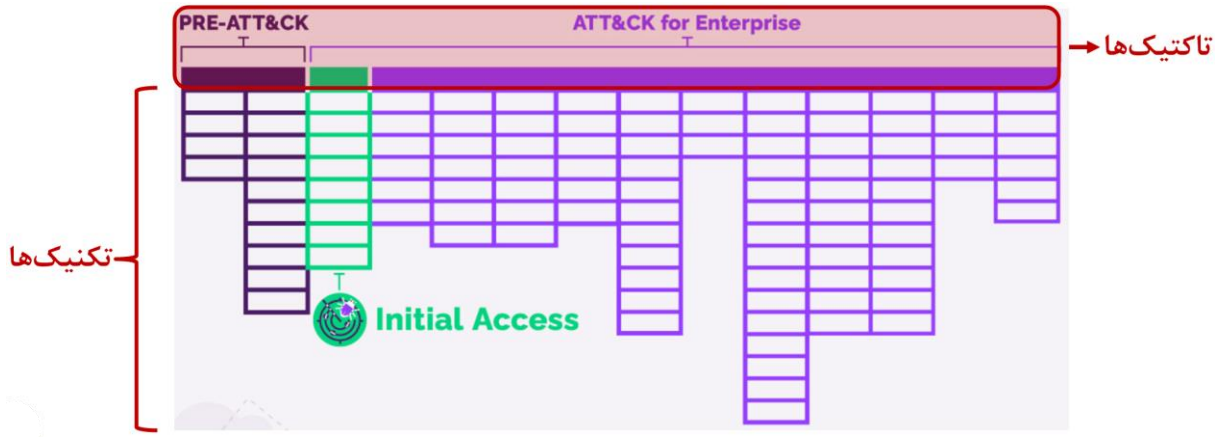
در سطح بالا، ATT&CK یک مدل رفتاری است که شامل تاکتیک‌ها، تکنیک‌ها، استفاده مهاجمین از تکنیک‌ها و رویه‌های آن‌ها و کاهش‌های مرتبط است. این چارچوب ابتدا فقط برای سیستم‌های ویندوزی ایجاد شد، اما از آن زمان به سیستم‌های Linux، Mac OS، Mobile، Cloud و حتی سیستم‌های ICS گسترش یافته است. MITRE سه دامنه فناوری را برای تطبیق با این تغییر ایجاد کرد. این دامنه‌ها که سکوهای مختلف را گروه‌بندی می‌کنند در جدول ۱ نشان داده شده است.

[۱] https://attack.mitre.org

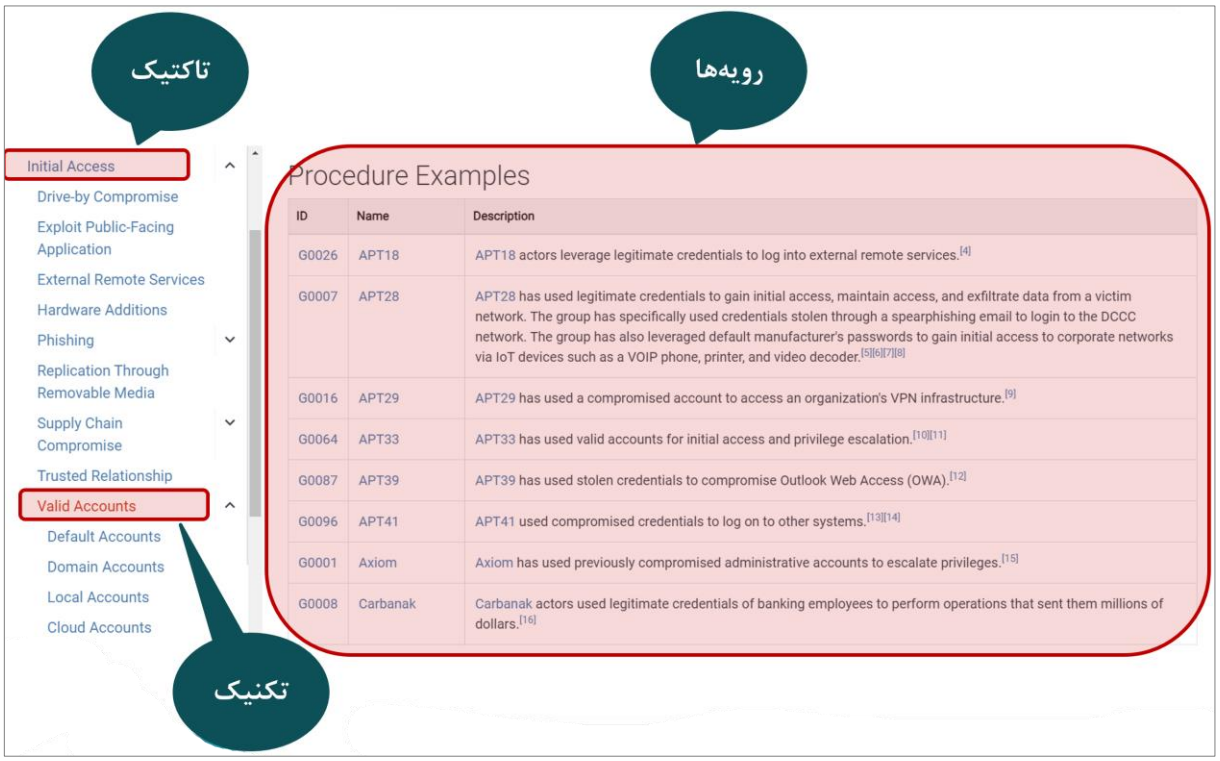
جدول ۱- دامنه‌های فناوری ارائه‌شده توسط MITRE ATT&CK

دامنه فناوری	سکو
Enterprise	Windows, Linux, Mac Os, Azure AD, AWS, GCP
Mobile	Android, iOS
ICS	SCADA systems, PLCs, HMIs

ماتریس ATT&CK یک نمایش بصری از رابطه بین تاکتیک‌ها، تکنیک‌ها و تکنیک‌های فرعی است. برای هر حوزه فناوری یک ماتریس وجود دارد. شِمای کلی این ماتریس در شکل ۱۲ نشان داده شده است. به عنوان یک مثال واقعی، شکل ۱۳ یکی از تاکتیک‌های موجود در ماتریس ATT&CK را به‌همراه یکی از تکنیک‌های رسیدن به آن و همچنین برخی رویه‌های استفاده‌شده برای این تکنیک در دنیای واقعی را نشان می‌دهد.



شکل ۱۲ شِمای کلی ماتریس MITRE ATT&CK



شکل ۱۳ مفهوم تاکتیک، تکنیک و رویه در MITRE ATT&CK

۳-۲-۱ تاکتیک‌ها

تاکتیک‌ها دستاوردهای تاکتیکی هستند که مهاجم هنگام انجام یک عمل به آن‌ها می‌پردازد. تاکتیک دلیل پشت آن عمل است. به عبارت دیگر، وقتی بازیگران بدخواه از تکنیک‌ها استفاده می‌کنند، تاکتیک همان چیزی است که می‌خواهند به آن برسند. به عنوان مثال، دانلودهای Drive-by تکنیکی برای رسیدن به هدف تاکتیکی دسترسی اولیه به یک سیستم است. تاکتیک‌های فعلی در MITER ATT&CK برای دامنه سازمانی[۱] عبارتند از:

- **شناسایی:** این مرحله جایی است که مهاجم به تحقیق، شناسایی و جمع‌آوری اطلاعات در مورد هدف می‌پردازد. اطلاعات را می‌توان با هر وسیله‌ای، فعال و غیرفعال به‌دست آورد. به عنوان مثال، ابزارهای OSINT مانند Maltego/Shodan، SIGINT، HUMINT و غیره.
- **توسعه منابع:** طراحی، جمع‌آوری و اجرای منابع برای پشتیبانی از عملیات. به عنوان مثال، راه‌اندازی یک بات‌نت یا یک زیرساخت C۲.
- **دسترسی اولیه:** به‌دست‌آوردن جای پایی در شبکه هدف. به عنوان مثال، دانلودهای Drive-by یا فیشینگ.

[۱] Enterprise

- **اجرا:** اجرای کدهای مخرب در دستگاه مورد دسترسی. به عنوان مثال، تلاش برای راه‌اندازی ابزار دسترسی از راه دور.
- **ماندگاری[۱]:** اطمینان از حفظ حضور در شبکه برای استفاده مجدد در آینده. به عنوان مثال، تغییر تنظیمات سیستم.
- **افزایش امتیاز[۲]:** تلاش برای دریافت مجوزهای بالاتر. به عنوان مثال، دسترسی کاربر ریشه در ماشین لینوکس یا نقش مدیر سیستم در ویندوز.
- **فرار از دفاع:** اجتناب از ابزارهای دفاعی که توسط مدافع در جای خود قرار داده شده است. به عنوان مثال، استتار بدافزار به عنوان نرم افزار قانونی.
- **دسترسی به اعتبارنامه:** دریافت اعتبارنامه حساب‌ها و کاربران. به عنوان مثال، Keylogging، Credential Dumping.
- **کشف:** نقشه‌برداری و درک محیط هدف. به عنوان مثال، کشف میزبان‌ها در شبکه یا پردازه‌های در حال اجرا در ماشین قربانی.
- **حرکت جانبی:** حرکت در داخل محیط هدف. به عنوان مثال، چرخش از یک ماشین به ماشین دیگر در داخل همان شبکه.
- **جمع‌آوری:** تا آنجا که ممکن است داده‌های مرتبط با مأموریت را کنار هم قرار دهید.
- **فرمان و کنترل:** ایجاد یک پل C۲ بین سیستم‌های قربانی و سرورهای فرمان و کنترل. به عنوان مثال، برقراری ارتباط با یک وب‌سایت C۲ با نام ناشناس در اینترنت از طریق درخواست‌های HTTP GET.
- **اکسفیلتراسیون[۳]:** انتقال داده در سراسر مرز شبکه هدف. به عنوان مثال. انتقال فیزیکی (از طریق دستگاه USB)، یا انتقال برنامه‌ریزی‌شده.
- **تأثیر:** آسیب به داده‌ها، وقفه در خدمات و فرآیندهای حیاتی در سیستم هدف. به عنوان مثال، پاک‌کردن دیسک، باج افزار.

تاکتیک‌های بالا یک لیست نامرتب را تشکیل می‌دهند و عناصر آن لزوماً روایت متوالی یک حمله را نشان نمی‌دهند. جدول ۲ خلاصه‌ای از این تاکتیک‌ها را نشان می‌دهد.

---

[۱] Persistence

[۲] Privilege Escalation

[۳] Exfiltration

جدول ۲ خلاصه‌ای از تاکتیک‌های موجود در MITRE ATT&CK

تاکتیک	در این تاکتیک مهاجم تلاش می‌کند که
شناسایی	اطلاعاتی را جمع‌آوری کند که بتواند از آن‌ها برای برنامه‌ریزی عملیات آینده استفاده کند
توسعه منابع	منابعی را ایجاد کند که بتواند از آن‌ها برای پشتیبانی از عملیات استفاده کند
دسترسی اولیه	وارد شبکه قربانی شود
اجرا	کدهای مخرب را اجرا کند
ماندگاری	جای پای خود را حفظ کند
افزایش امتیاز	مجوزهای سطح بالاتر را به دست آورد
فرار از دفاع	از شناسایی شدن جلوگیری کند
دسترسی به اعتبارنامه	نام و رمز عبور حساب‌ها را سرقت کند
کشف	محیط شبکه قربانی را کشف کند
حرکت جانبی	در محیط شبکه قربانی حرکت کند.
جمع‌آوری	داده‌های مورد علاقه خود را جمع‌آوری کند
فرماندهی و کنترل	با سیستم‌های در معرض خطر برای کنترل آن‌ها ارتباط برقرار کند
اکسفیلتراسیون	اطلاعات را سرقت کند
تأثیر	سیستم‌ها و داده‌های قربانی را دستکاری، قطع یا نابود کند

۳-۲-۲ تکنیک‌ها

در حالی‌که تاکتیک‌ها «چرایی» یک عمل را نشان می‌دهند، تکنیک‌ها «چگونگی» آن را نشان می‌دهند. به عنوان مثال، بهره‌برداری از یک برنامه کاربردی عمومی، تکنیکی است که برای رسیدن به تاکتیک دسترسی اولیه استفاده می‌شود. از آنجایی‌که تکنیک‌ها فقط ابزارهایی برای یک هدف هستند و ممکن است چندین ابزار برای رسیدن به یک هدف وجود داشته باشد، بسیاری از تکنیک‌ها را می‌توان در یک دسته تاکتیکی واحد گروه‌بندی کرد. شکل ۱۴ مثال کوچکی از این موضوع است: تاکتیک حرکت جانبی را می‌توان با استفاده از ۹ تکنیک مختلف انجام داد. هر تکنیک می‌تواند از یک یا چند تکنیک فرعی تشکیل شده باشد.

Techniques for the Lateral Movement Tactic
Exploitation of remote services
Internal spearphishing
Lateral tool transfer
Remote server session hijacking
Remote services
Replication through removable media
Software development tools
Taint shared content
Use alternate authentication material

شکل ۱۴ تکنیک‌های موجود در یک تاکتیک

۳-۲-۳ تکنیک‌های فرعی (زیرتکنیک‌ها)

تکنیک‌ها را می‌توان به رفتارهای خاص‌تری تقسیم کرد که برای به‌دست‌آوردن یک هدف تاکتیکی استفاده می‌شوند. این رفتارهای خاص‌تر را تکنیک‌های فرعی یا زیرتکنیک‌ها می‌نامند. از منظر طبقه‌بندی، یک تکنیک می‌تواند والد یک یا چند تکنیک فرعی باشد. تکنیک‌های فرعی در سال ۲۰۲۰ میلادی در تلاش MITRE برای حل چندین مسئله انتزاعی که به دلیل رشد سریع مدل رخ داد اضافه شدند. در واقع برخی از تکنیک‌های MITRE بیش از حد گسترده و برخی بیش از حد خاص بودند تا جایی که خواندن، تجسم، درک و نگهداری ماتریس ATT&CK را سخت می‌کرد. افزودن تکنیک‌های فرعی بسیاری از این مشکلات را برطرف کرد:

- سطح انتزاع کلی تکنیک‌ها عادی شد.
- تعداد تکنیک‌ها به سطحی کاهش یافت که خواندن، نگهداری و به‌روزرسانی آسان‌تر بود.
- نشان داد که یک تکنیک را می‌توان به روش‌های مختلف اجرا کرد.

شکل ۱۴ نشان داد که چگونه تکنیک‌ها تحت یک تاکتیک گروه‌بندی می‌شوند. شکل ۱۵ آن را گسترش می‌دهد تا تمام تکنیک‌های فرعی تکنیک خدمات از راه دور را شامل شود. برای درک آسان‌تر، تعریف MITRE ATT&CK از تکنیک خدمات از راه دور عبارت است از: «مهاجمین ممکن است از حساب‌های معتبر برای ورود به سرویسی استفاده کنند که به طور خاص برای پذیرش اتصالات راه دور طراحی شده است، مانند Telnet، SSH و VNC. سپس مهاجم ممکن است به عنوان کاربر وارد شده اقداماتی را انجام دهد.»

Techniques for the Lateral Movement Tactic
Exploitation of remote services
Internal spearphishing
Lateral tool transfer
Remote server session hijacking
Remote services
Sub-techniques for the Remote service Technique
Remote Desktop Protocol
SMB/Windows Admin Shares
Distributed Component Object Model
SSH
VNC
Windows Remote Management
Replication through removable media
Software development tools
Taint shared content
Use alternate authentication material

شکل ۱۵ زیرتکنیک‌های موجود در یک تکنیک

RDP، SMB، SSH، VNC، مدیریت از راه دور ویندوز و مدل COM ویندوز، همگی از تکنیک‌های فرعی ممکن در تکنیک خدمات از راه دور هستند که برای دستیابی به تاکتیک حرکت جانبی استفاده می‌شوند.

۳-۲-۴ رویه‌ها

رویه‌ها نشان می‌دهند که مهاجمین خاص چگونه تکنیک‌های مختلف را اجرا می‌کنند. روش کار و ابزار آن‌ها در رویه‌ها ذکر شده است. به عنوان مثال برای دستیابی به هدف تاکتیکی C۲ می‌توان از تکنیک‌ها و تکنیک‌های فرعی بسیاری استفاده کرد. یکی از گروه‌های تکنیکی بر استفاده از پروتکل(های) لایه کاربرد تکیه دارد که در آن عوامل مخرب سعی می‌کنند یک پل C۲ را با ترکیب کردن ترافیک موجود و مجاز در لایه کاربرد ایجاد کنند.

گروه‌های تهدید پیشرفته مختلف از روش‌های مختلفی برای دستیابی به هدف تاکتیکی این تکنیک استفاده می‌کنند:

- Cobalt Strike از P۲P روی لوله‌های[۱] نامگذاری شده ویندوز در پروتکل SMB استفاده می‌کند.
- Rocke برای ایجاد درخواست‌های wget برای رسیدن به سرور C۲ استفاده می‌شود.

[۱] Pipes

- خانواده‌های بدافزار Magic Hound از IRC برای ایجاد یک کانال C۲ استفاده کرده‌اند.
- APT۱۸ (همچنین به نام Dynamite Panda یا ۰۴۱۶ Threat Group نیز شناخته می‌شود) به دلیل استفاده از پرس‌وجوهای DNS TXT برای برقراری ارتباط با سرور C۲ خود به خوبی شناخته شده است.

۳-۲-۵ گروه‌ها

هنگامی‌که گزارش‌های هوش تهدیدات عمومی یا خصوصی، فعالیت‌های متخاصم را مستند می‌کنند، گروه‌های تهدید پشت این فعالیت‌ها تحت هدف Groups در چارچوب ردیابی می‌شوند. گروه‌ها یا گروه‌های تهدید، بازیگران تهدید، مجموعه‌های نفوذ یا خانواده‌های بدافزاری هستند که فعالیت‌های هدفمند، پیشرفته و مداوم را انجام می‌دهند. به عنوان مثال، APT۲۹ یک گروه است و RYUK نیز یک گروه است.

۳-۲-۶ نرم‌افزار

مجموعه‌ای از تمام نرم‌افزارهایی است که می‌توان از آن‌ها برای اجرای تکنیک‌های خاص برای دستیابی به اهداف تاکتیکی مستند MITRE ATT&CK استفاده کرد. نرم‌افزارها به دو زیرگروه کلان تقسیم می‌شوند: ابزارها و بدافزارها. زیرگروه اول شامل نرم‌افزارهای تجاری یا داخلی است که می‌تواند توسط مهاجمان و مدافعان به طور یکسان استفاده شود و ممکن است به طور پیش‌فرض در اکثر سیستم‌های سازمانی یافت شود. به عنوان مثال، PS Exec، ابزارهای ویندوز و wget. زیرگروه دوم حاوی نرم‌افزارهایی است که فقط توسط عوامل مخرب برای اهداف مخرب استفاده می‌شود. به عنوان مثال، FakeInstaller و DroidKungFu. این تقسیم‌بندی به نرم‌افزارهای مخرب و غیرمخرب به این دلیل در نظر گرفته شده است که نشان دهد که چگونه می‌توان از نرم‌افزارهای قانونی برای نفوذ به همان اندازه نرم‌افزارهای غیرقانونی استفاده کرد.

۳-۲-۷ اقدامات کاهشی[۱]

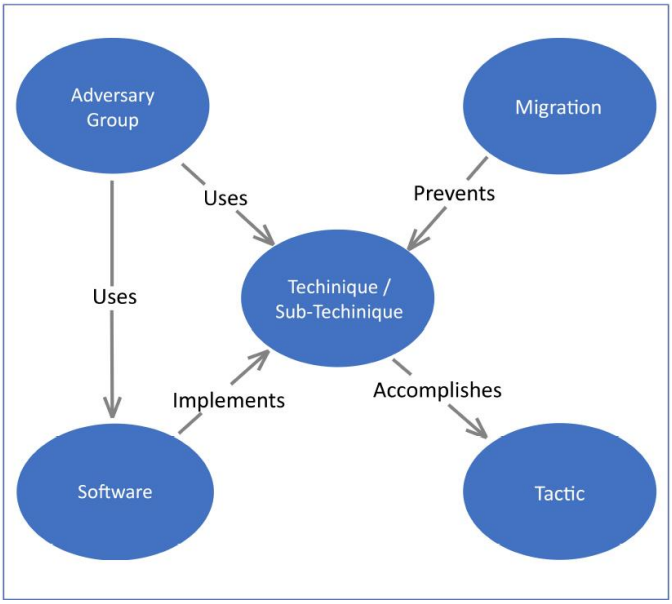
مجموعه‌ای از تمام کنترل‌ها، حفاظت‌ها و اقدامات متقابلِ شناخته‌شده است که می‌تواند برای جلوگیری از اجرای موفقیت‌آمیز تکنیک‌ها (و تکنیک‌های فرعی) اعمال شود. در ادامه چند نمونه با توضیحی کوتاه آورده شده است.

- راهنمای توسعه‌دهنده برنامه: توسعه‌دهندگانی که برای کدنویسی دفاعی آموزش دیده‌اند تا از به‌وجودآمدن آسیب‌پذیری‌ها در برنامه‌های خود جلوگیری کنند.
- تقسیم‌بندی شبکه: جداسازی سیستم‌ها و منابع حیاتی، به صورت منطقی، فیزیکی یا هر دو. به عنوان مثال، DMZها و VPCها.
- آموزش کاربر: برنامه‌های آموزشی آگاهی از امنیت.

[۱] Mitigations

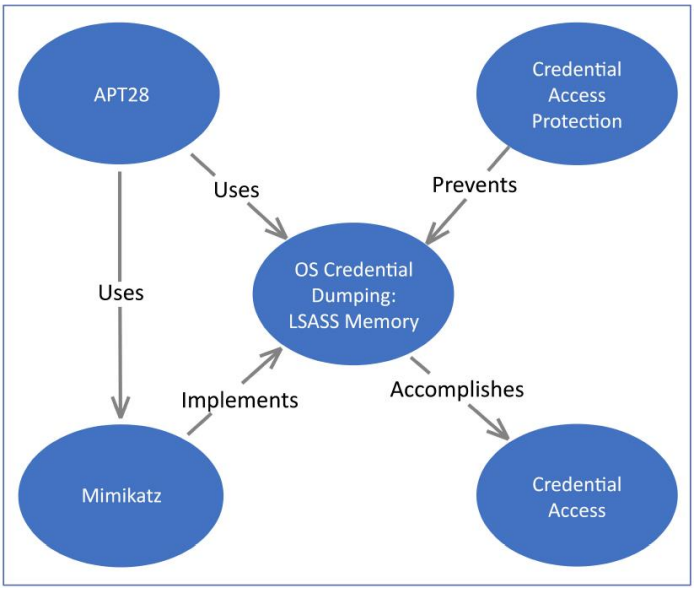
۳-۲-۸ تعامل اشیاء در MITER ATT&CK

اشیائی که در بخش‌های قبل مورد بررسی قرار گرفتند همگی با یکدیگر تعامل دارند. درک اینکه چگونه تاکتیک‌ها، تکنیک‌ها، رویه‌ها، اقدامات کاهشی، گروه‌ها و نرم‌افزار با یکدیگر ارتباط دارند برای استفاده صحیح از چارچوب بسیار مهم است. شکل ۱۶ تعامل این اشیاء را در یک سطح کلی توصیف می‌کند.



شکل ۱۶ تعامل اشیای موجود در MITRE ATT&CK با یکدیگر

شکل ۱۷ یک مثال واقعی از نمونه قبلی را نشان می‌دهد. رفتار APT۲۸ (Fancy Bear) مورد تحلیل قرار گرفته و نشان می‌دهد که چگونه از credential dumping از طریق نرم‌افزار (Mimikatz) برای دستیابی به دسترسی به اعتبارنامه استفاده می‌کند.



شکل ۱۷ تعامل اشیای موجود در MITRE ATT&CK با یکدیگر در APT۲۸

۳-۲-۹ مهم‌ترین عناصر موجود در MITRE ATT&CK

در جمع‌بندی و خلاصه‌ای از مباحث ارائه‌شده در این بخش می‌توان بیان کرد که تاکتیک، تکنیک، منبع داده، مؤلفه داده و روش شناسایی مهم‌ترین عناصر موجود در MITRE ATT&CK هستند. جداول ۳ و ۴ دو تکنیک مربوط به دو تاکتیک مختلف از MITRE ATT&CK را نشان می‌دهند. در این جداول تکنیک‌های فرعی مورد استفاده نیز قابل مشاهده است. جمع‌آوری اطلاعات مربوط به منبع داده و مؤلفه داده می‌تواند دید خوبی در زمینه منابع داده پر کاربرد در حملات و تهدیدات سایبری واقعی ارائه دهد. همچنین جمع‌آوری اطلاعات مربوط به شناسایی می‌تواند کمک قابل توجهی به ارتقای سطح تشخیص تهدیدات در سکوی هوش تهدید نماید.

جدول ۳ مهم‌ترین عناصر موجود در MITRE ATT&CK در تکنیک اسکن فعال از تاکتیک شناسایی

شناسایی	مؤلفه داده	منبع داده	تکنیک فرعی	تکنیک	تاکتیک
نظارت بر داده‌های شبکه برای جریان‌های داده غیرمعمول. پردازه‌هایی که از شبکه استفاده می‌کنند و معمولاً ارتباط شبکه‌ای ندارند یا قبلاً هرگز دیده نشده‌اند مشکوک هستند.	جریان ترافیک شبکه	ترافیک شبکه	اسکن بلاک‌های IP	اسکن فعال	شناسایی
نظارت و تحلیل الگوهای ترافیک و بازرسی بسته‌های مرتبط با پروتکل‌هایی که از استانداردهای پروتکل مورد انتظار و جریان‌های ترافیک پیروی نمی‌کنند.	محتوای ترافیک شبکه	ترافیک شبکه	اسکن آسیب‌پذیری		
نظارت بر داده‌های شبکه برای جریان‌های داده غیرمعمول. پردازه‌هایی که از شبکه استفاده می‌کنند و معمولاً ارتباط شبکه‌ای ندارند یا قبلاً هرگز دیده نشده‌اند مشکوک هستند.	جریان ترافیک شبکه				
نظارت بر ترافیک شبکه مشکوک که می‌تواند نشان‌دهنده اسکن باشد، مانند مقادیر زیادی که از یک منبع منشا می‌گیرند (مخصوصاً اگر منبع شناخته‌شده با یک مهاجم/ باتنت مرتبط است).	محتوای ترافیک شبکه	ترافیک شبکه	اسکن لیست کلمات		

جدول ۴ مهم‌ترین عناصر موجود در MITRE ATT&CK در تکنیک ایجاد حساب از تاکتیک ماندگاری

شناسایی	مؤلفه داده	منبع داده	تکنیک فرعی	تکنیک	تاکتیک
نظارت بر دستورات و آرگومان‌های اجراشده برای اقدامات مرتبط با ایجاد حساب محلی، مانند net user /add، useradd و dscl -create	اجرای دستور	دستور	حساب محلی	ایجاد حساب	ماندگاری
نظارت بر پردازه‌های جدید اجراشده مرتبط با ایجاد حساب، مانند net.exe.	ایجاد پردازه	پردازه			
برای شناسایی حساب‌های مشکوک که ممکن است توسط مهاجم ایجاد شده باشد، حساب‌های کاربری جدید ساخته شده را از طریق ممیزی حساب کنترل کنید. جمع‌آوری داده‌ها در مورد ایجاد حساب در یک شبکه یا Windows Event ID ۴۷۲۰ (برای زمانی که یک حساب کاربری در سیستم ویندوز و DC ایجاد می‌شود).	ایجاد حساب کاربر	حساب کاربر			

نظارت بر دستورات و آرگومان‌های اجراشده برای اقداماتی که با ایجاد حساب محلی مرتبط هستند، مانند net user /add /domain.	اجرای دستور	دستور	حساب دامنه		
نظارت بر پردازه‌های جدید اجراشده مرتبط با ایجاد حساب، مانند net.exe	ایجاد پردازه	پردازه			
.....	ایجاد حساب کاربر	حساب کاربر			
برای شناسایی فعالیت‌های غیرمعمول در ایجاد حساب‌های جدید، مانند حساب‌هایی که از قراردادهای نام‌گذاری مشخص یا حساب‌های ایجاد شده توسط کاربران یا منابع تأیید نشده پیروی نمی‌کنند، بر حساب‌های کاربری تازه‌ساخته‌شده را از طریق مجموعه‌ای از لاگ‌های استفاده از حساب‌های کاربر ابری و ادمین نظارت کنید. بر حساب‌های مدیریت جدید ایجاد شده که از آستانه مشخصی از ادمین‌های شناخته‌شده فراتر می‌روند نظارت کنید.	ایجاد حساب کاربر	حساب کاربر	حساب ابری		

۳-۳ ارتباط MITRE ATT&CK و ENISA Threat Landscape

۳-۳-۱ ENISA Threat Landscape ۲۰۲۲

ENISA Threat Landscape ۲۰۲۲[۱] دهمین ویرایش گزارش چشم‌انداز تهدید ENISA است، گزارشی سالانه درباره وضعیت چشم‌انداز تهدید امنیت سایبری. این گزارش تهدیدات، روندهای اصلی مشاهده‌شده با توجه به تهدیدات، عوامل تهدید و تکنیک‌های حمله و همچنین تحلیل تأثیر و انگیزه مهاجم را شناسایی کرده، اقدامات کاهشی مربوطه را تشریح می‌کند. در طول سال ۲۰۲۲ میلادی تهدیدهای اصلی شناسایی‌شده توسط ENISA عبارتند از (شکل ۱۸):

۱. باج‌افزار
۲. بدافزار
۳. تهدیدات مهندسی اجتماعی
۴. تهدید علیه داده‌ها
۵. تهدید علیه در دسترس بودن: انکار سرویس
۶. تهدید علیه در دسترس بودن: تهدیدات اینترنتی
۷. اطلاعات نادرست
۸. حملات زنجیره تأمین

[۱] https://www.enisa.europa.eu/publications/enisa-threat-landscape-۲۰۲۲

شکل ۱۸ تهدیدات اصلی شناسایی‌شده توسط ENISA Threat Landscape در سال ۲۰۲۲

۳-۳-۲ نگاشت ENISA Threat Landscape به MITRE ATT&CK

ENISA Threat Landscape در نسخه‌های اخیر خود نگاشت تهدیدات شناسایی‌شده توسط خود به MITRE ATT&CK را ارائه می‌دهد. به‌عنوان مثال شکل ۱۹ بخشی از جدول نگاشت تهدیدات دسته‌ی اطلاعات نادرست از ENISA Threat Landscape به MITRE ATT&CK را ارائه می‌دهد.

DISINFORMATION - MISINFORMATION	
It is important to note that disinformation and misinformation attacks are among the preparatory activities at the basis of other attacks (e.g. phishing, social engineering, malware infection). The MITRE ATT&CK® graph below can give an idea of the link between disinformation/misinformation and connected attacks.	
TA0043: Reconnaissance	T1592: Gather Victim Host Information T1589: Gather Victim Identity Information T1590: Gather Victim Network Information T1591: Gather Victim Org Information T1598: Phishing for Information T1597: Search Closed Sources T1596: Search Open Technical Databases T1593: Search Open Websites/Domains T1594: Search Victim-Owned Websites
TA0042: Resource Development	T1586: Compromise Accounts T1585: Establish Accounts
TA0001: Initial Access	T1566: Phishing
TA0002: Execution	T1203: Exploitation for Client Execution T1204: User Execution
TA0040: Impact	T1565: Data Manipulation T1491: Defacement

شکل ۱۹ بخشی از جدول نگاشت تهدیدات دسته‌ی اطلاعات نادرست از ENISA Threat Landscape به MITRE ATT&CK

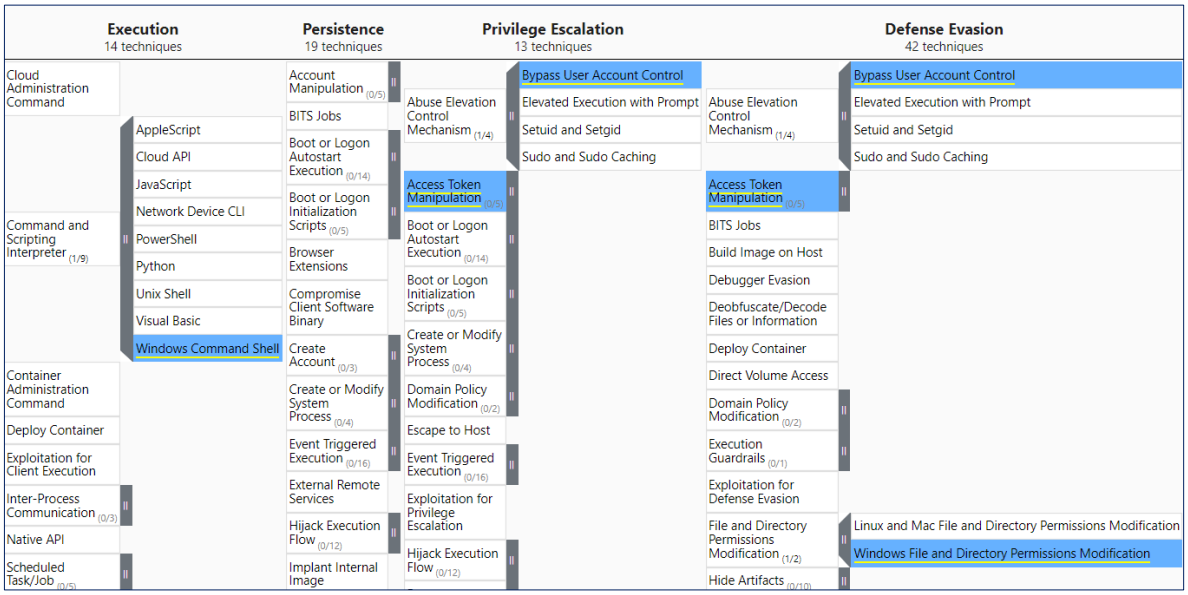
۳-۴ نگاشت MITRE ATT&CK به سناریوهای واقعی تهدید

در این بخش به‌عنوان مثال‌های واقعی دو سناریوی واقعی تهدید (BlackCat[۱] و APT۲۹[۲]) مورد مطالعه قرار گرفته و نگاشت MITRE ATT&CK به آن‌ها بررسی می‌شود.

۳-۴-۱ BlackCat

BlackCat باج‌افزار نوشته‌شده به زبان Rust است که از طریق مدل Ransomware-as-a-Service (RaaS) ارائه شده است. این باج‌افزار برای اولین بار در نوامبر سال ۲۰۲۱ میلادی مشاهده شد. BlackCat برای هدف قرار دادن چندین بخش و سازمان در کشورها و مناطق مختلف در آفریقا، آمریکا، آسیا، استرالیا و اروپا استفاده شده است.

شکل ۲۰ برخی تکنیک‌های MITRE ATT&CK که توسط BlackCat استفاده شده‌اند را نشان می‌دهد. جدول ۶ این تکنیک‌ها را به‌صورت کامل نشان داده و به‌صورت کوتاه در مورد روش استفاده BlackCat از آن‌ها توضیح می‌دهد.



شکل ۲۰ برخی تکنیک‌های MITRE ATT&CK که توسط BlackCat استفاده شده‌اند

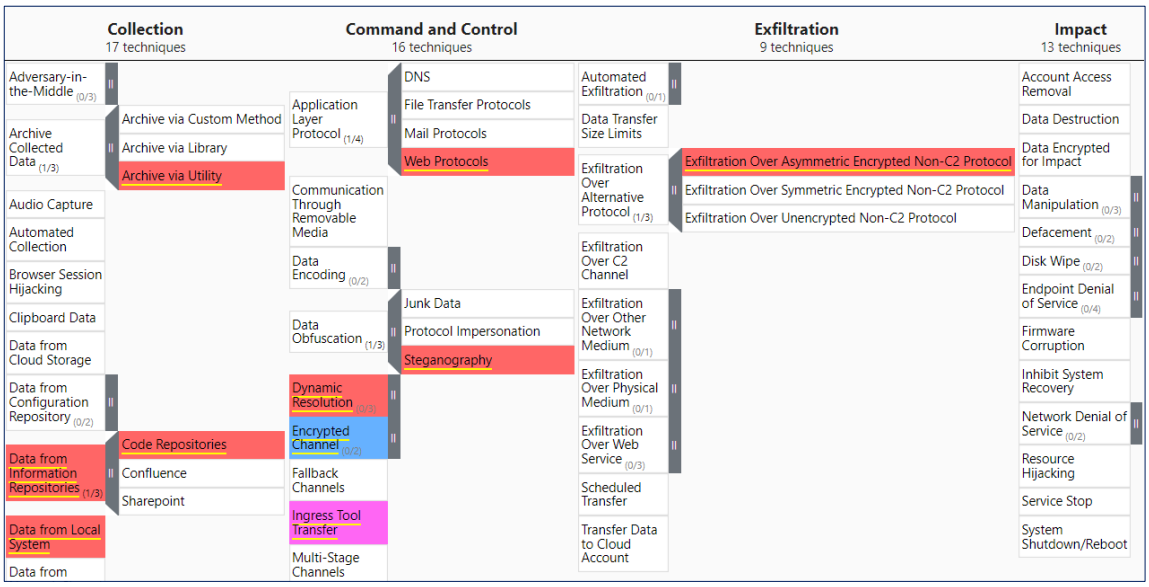
۳-۴-۲ APT۱۹

APT۱۹ یک گروه تهدید مستقر در چین است که صنایع مختلفی از جمله دفاعی، مالی، انرژی، داروسازی، مخابرات، فناوری پیشرفته، آموزش، تولید و خدمات حقوقی را هدف قرار داده است. در سال ۲۰۱۷ میلادی یک کمپین فیشینگ برای هدف قرار

[۱] https://attack.mitre.org/software/S۱۰۶۸/
[۲] https://attack.mitre.org/groups/G۰۰۱۶/

دادن هفت شرکت حقوقی و سرمایه‌گذاری مورد استفاده قرار گرفت. برخی از تحلیلگران APT۱۹ و Deep Panda را به عنوان یک گروه دنبال می‌کنند، اما اطلاعات منبع باز مشخص نیست که آیا گروه‌ها یکسان هستند یا خیر.

شکل ۲۱ برخی تکنیک‌های MITRE ATT&CK که توسط APT۱۹ استفاده شده‌اند را نشان می‌دهد. جدول ۷ این تکنیک‌ها را به‌صورت کامل نشان داده و به‌صورت کوتاه در مورد روش استفاده APT۱۹ از آن‌ها توضیح می‌دهد.



شکل ۲۱ برخی تکنیک‌های MITRE ATT&CK که توسط APT۱۹ استفاده شده‌اند

۳-۵ استفاده از MITRE ATT&CK برای هوش تهدید

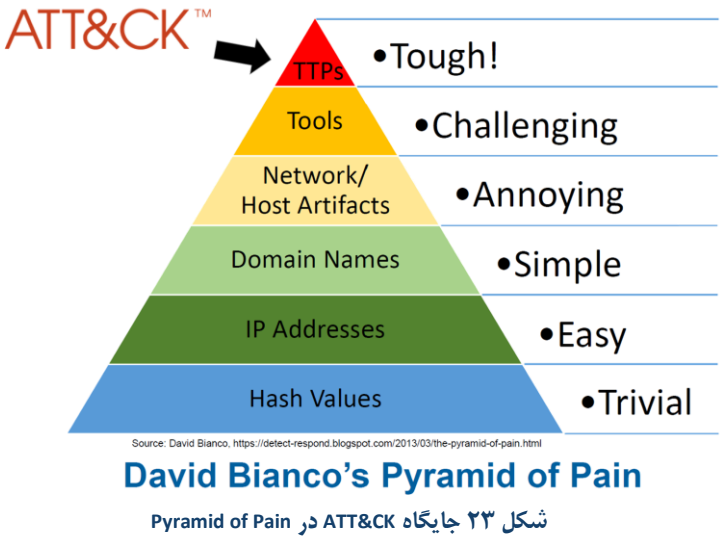
روال استفاده از MITRE ATT&CK در هوش تهدید سایبری به پنج ماژول نشان داده شده در شکل ۲۲ شکسته می‌شود[۱]. در ادامه در مورد هر یک از این ماژول‌ها توضیحاتی ارائه می‌شود.

شکل ۲۲ روال استفاده از MITRE ATT&CK در هوش تهدید سایبری

[۱] https://attack.mitre.org/resources/training/

۳-۵-۱ ماژول ۱: درک ATT&CK

هدف از ATT&CK استفاده از دانش رفتارهای مهاجم برای آگاه‌کردن مدافعان است. ساختار هوش تهدید با ATT&CK به ما این امکان را می‌دهد که رفتار گروه‌ها را با یکدیگر و در طول زمان مقایسه کرده و با یک زبان مشترک ارتباط برقرار کنیم. همان‌طور که در شکل ۲۲ مشاهده می‌شود، کار اصلی ATT&CK استخراج TTPها است که دانش بسیار ارزشمندی برای کمک به هوش تهدید سایبری می‌باشد.



شکل ۲۳ جایگاه ATT&CK در Pyramid of Pain

۳-۵-۲ ماژول‌های ۲ و ۳: نگاشت به ATT&CK

دو منبع کلیدی برای دریافت اطلاعات عبارتند از:

- گزارش خاتمه‌یافته
- داده‌های خام

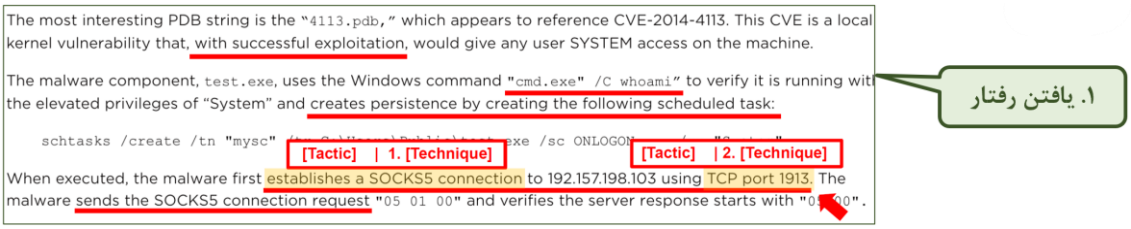
در حالت کلی فرایند نگاشت به ATT&CK شامل پنج مرحله زیر است:

۱. یافتن رفتار
۲. تحقیق و جست‌وجو در مورد رفتار
۳. ترجمه رفتار به تاکتیک
۴. یافتن تکنیک اعمال‌شده به رفتار
۵. مقایسه نتایج با دیگر تحلیلگران

۳-۵-۲-۱ *ماژول ۲: نگاشت به ATT&CK از گزارش خاتمه‌یافته*

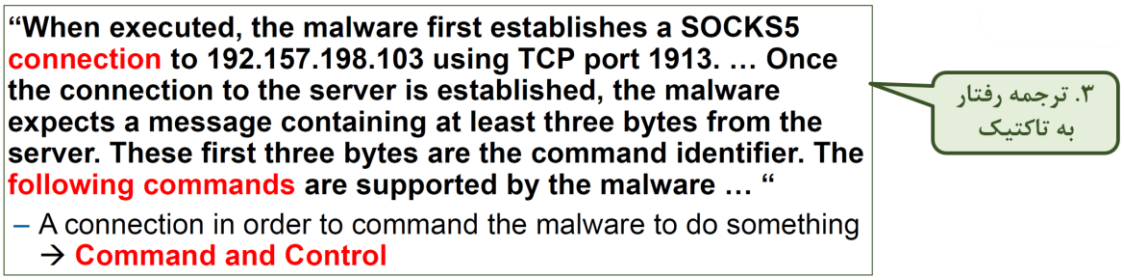
شکل‌های ۲۴ تا ۲۷ با یک مثال فرایند نگاشت به ATT&CK از گزارش خاتمه‌یافته را نشان می‌دهد. همان‌طور که در این شکل‌ها مشاهده می‌شود این فرایند از یک گزارش خاتمه‌یافته شروع شده و با بررسی دقیق نزدیک‌ترین رفتارها به آن استخراج می‌شود. سپس به تحقیق و جست‌وجو در مورد رفتارهای استخراج‌شده از طریق منابع عمومی (و در صورت امکان منابع غیرعمومی)

پرداخته می‌شود. پس از اتمام تحقیق و جست‌وجو، رفتارهای یافته‌شده در مرحله اول به نزدیک‌ترین تاکتیک‌های متناظر در ATT&CK ترجمه شده و در نهایت تکنیک اعمال‌شده به رفتار (از مجموعه تکنیک‌های دسته‌ی تاکتیک استخراج‌شده در مرحله قبل) پیدا می‌شود.

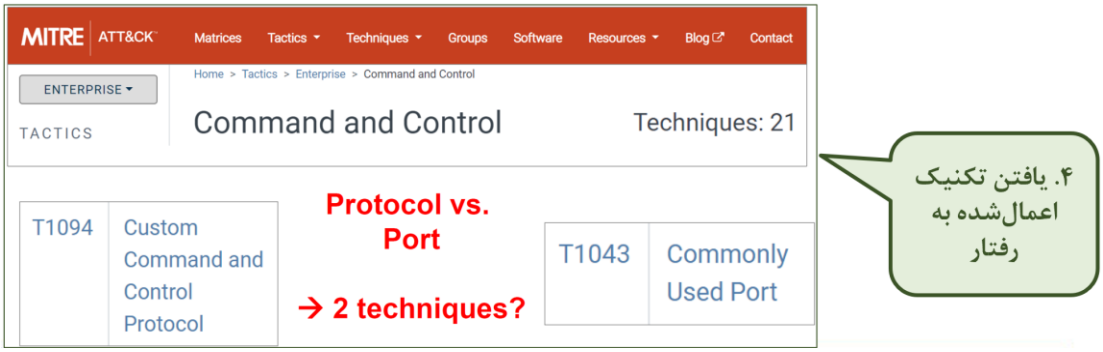


شکل ۲۴ نگاشت به ATT&CK از گزارش خاتمه‌یافته– مرحله یافتن رفتار

شکل ۲۵ نگاشت به ATT&CK از گزارش خاتمه‌یافته– مرحله تحقیق و جست‌وجو در مورد رفتار



شکل ۲۶ نگاشت به ATT&CK از گزارش خاتمه‌یافته– مرحله ترجمه رفتار به تاکتیک



شکل ۲۷ نگاشت به ATT&CK از گزارش خاتمه‌یافته- مرحله یافتن تکنیک اعمال‌شده به رفتار

۳-۵-۲-۲ ماژول ۳: نگاشت به ATT&CK از داده خام

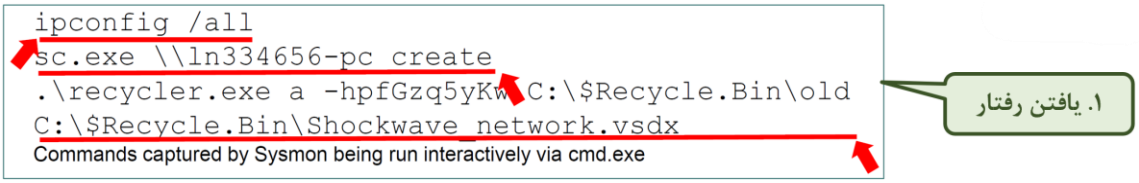
در این ماژول تحلیل تکنیک‌ها/رفتارها به طور مستقیم از داده‌های منبع مورد بررسی قرار می‌گیرد (به‌جای گزارش خاتمه‌یافته):

- با این روش احتمالاً اطلاعات بیشتری در سطح رویه (procedure) در دسترس است.
- در این روش نیاز به تفسیر مجدد نتایج یک تحلیلگر یا گزارش دیگر نیست.
- در این روش دانش/تخصص بیشتری برای تفسیر هدف/تاکتیک مورد نیاز است.

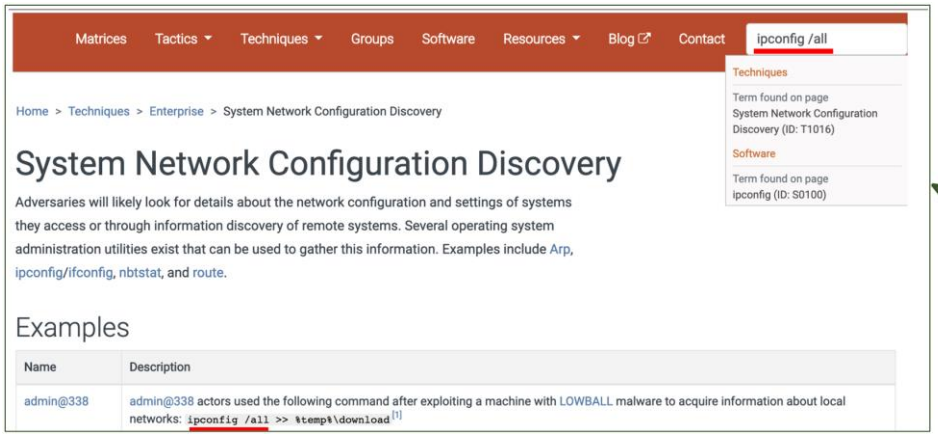
مجموعه گسترده‌ای از داده‌ها می‌توانند شامل رفتارها باشند:

- مانند: دستورات shell، بدافزار، فارنزیک تصاویر دیسک، بسته‌ها

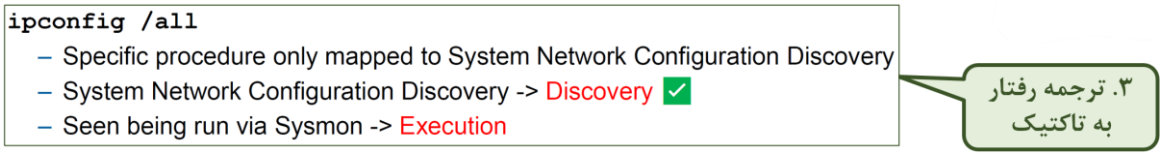
شکل‌های ۲۸ تا ۳۳ با یک مثال فرایند نگاشت به ATT&CK از داده خام را نشان می‌دهد. همان‌طور که در این شکل‌ها مشاهده می‌شود این فرایند از داده‌های خام شروع شده و با بررسی دقیق این داده‌ها رفتارهای موجود در آن‌ها استخراج می‌شود. سپس به تحقیق و جست‌وجو در مورد رفتارهای استخراج‌شده از طریق منابع عمومی (و در صورت امکان منابع غیرعمومی) پرداخته می‌شود. پس از اتمام تحقیق و جست‌وجو، رفتارهای یافته‌شده در مرحله اول به نزدیک‌ترین تاکتیک‌های متناظر در ATT&CK ترجمه شده و سپس تکنیک اعمال‌شده به رفتار (از مجموعه تکنیک‌های دسته‌ی تاکتیک استخراج‌شده در مرحله قبل) پیدا می‌شود. در نهایت بهتر است به مقایسه‌ی نتایج به‌دست‌آمده با دیگر تحلیلگران پرداخته شود. این مقایسه می‌تواند نتایج را به سمت دقیق‌تری هدایت کند.



شکل ۲۸ نگاشت به ATT&CK از داده خام- مرحله یافتن رفتار

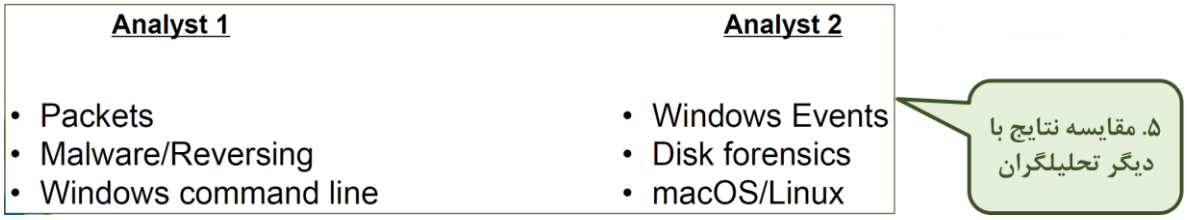


شکل ۲۹ نگاشت به ATT&CK از داده خام- مرحله تحقیق و جست‌وجو در مورد رفتار



شکل ۳۰ نگاشت به ATT&CK از داده خام- مرحله ترجمه رفتار به تاکتیک

شکل ۳۱ نگاشت به ATT&CK از داده خام- مرحله یافتن تکنیک اعمال‌شده به رفتار



شکل ۳۲ نگاشت به ATT&CK از داده خام- مرحله مقایسه نتایج با دیگر تحلیلگران

۳-۵-۳ ماژول ۴: ذخیره‌سازی و تحلیل ATT&CK-داده‌های نگاشت‌شده

توصیه‌های زیر را می‌توان برای ذخیره‌سازی در نظر گرفت:

- چه کسی آن را مصرف می‌کند؟
  - انسان یا ماشین؟
  - الزامات؟

- چگونه زمینه را فراهم خواهید کرد؟
- چقدر مفصل خواهد بود؟
  - فقط تکنیک ذخیره شود یا رویه را هم دربرگیرد؟
  - چگونه جزئیات را ثبت خواهید کرد؟
- چگونه آن را به هوش‌های دیگر پیوند می‌دهید؟
  - حادثه، گروه، شاخص و غیره
- چگونه داده‌ها را import و export می‌کنید؟
  - فرمت؟

۳-۵-۴ ماژول ۵: ایجاد توصیه‌های دفاعی از ATT&CK- داده‌های نگاشت‌شده

تمرکز کار در این ماژول بر عملی‌کردن هوش است (Actionable intelligence). فرایند ایجاد توصیه‌ها از تکنیک‌ها به‌صورت زیر است:

۱. اولویت تکنیک‌ها را تعیین کنید.
- روش‌های مختلف اولویت‌بندی
  - منابع داده: از قبل چه داده‌هایی دارید؟
  - هوش تهدید: مهاجمین شما چه می‌کنند؟
  - ابزارها: ابزارهای فعلی شما چه چیزی را می‌تواند پوشش دهد؟
  - تیم قرمز: تیم‌های قرمز در حال انجام چه کاری هستند؟

۲. تحقیق کنید که چگونه از تکنیک‌ها استفاده می‌شود.
- چه رویه‌های خاصی برای یک تکنیک معین استفاده می‌شود؟
  - مهم است که پاسخ دفاعی با فعالیت هم‌پوشانی داشته باشد

۳. در مورد گزینه‌های دفاعی مربوط به تکنیک‌ها تحقیق کنید.
- منابع زیادی وجود دارند که اطلاعات دفاعی نمایه‌شده به ATT&CK را ارائه می‌دهند، مهم‌ترین این منابع عبارتند از:
  - ATT&CK
    - Data Sources
    - Detections
    - Mitigations
    - لینک‌های تحقیقاتی موجود در صفحات مربوط به تکنیک‌ها
  - MITRE Cyber Analytics Repository (CAR)

- https://car.mitre.org
  - Roberto Rodriguez’s ThreatHunter Playbook
    - https://github.com/hunters-forge/ThreatHunter-Playbook
  - Atomic Threat Coverage
    - https://www.malwarearchaeology.com/cheat-sheets

۴. در مورد قابلیت‌ها/محدودیت‌های سازمان تحقیق کنید.
   - چه منابع داده یا تکنیک‌های دفاعی در حال حاضر در سازمان جمع‌آوری شده است؟
   - چه محصولاتی در حال حاضر در سازمان مستقر شده‌اند که امکان افزایش قابلیت‌ها در آن‌ها وجود داشته باشد؟
   - آیا چیزی در مورد سازمان وجود دارد که ممکن است مانع از پاسخ‌گویی به تهدیدات شود؟
۵. تعیین کنید که چه tradeoffهایی برای سازمان در گزینه‌های خاص وجود دارد.
   - چگونه هر یک از گزینه‌های دفاعی شناسایی‌شده در سازمان شما اعمال شوند؟
   - چه مزایا و معایبی در اعمال آن‌ها به سازمان شما وجود دارد؟
   - این مرحله به شدت به سازمان وابسته است.
۶. توصیه‌ها را ارائه کنید.
   - توصیه ممکن است از نوع فنی، تغییر سیاست یا پذیرش ریسک باشد.
   - توصیه ممکن است برای بخش مدیریت، SOC، IT یا همه این موارد باشد.
   - برخی از انواع توصیه‌ها عبارتند از:
     - فنی
       - جمع‌آوری منابع داده جدید
       - نوشتن یک تشخیص/تحلیل از داده‌های موجود
       - تغییر پیکربندی/تغییرات مهندسی
       - ابزار جدید
     - تغییر سیاست
       - فنی/انسانی
     - پذیرش ریسک
       - برخی تهدیدات غیرقابل تشخیص/غیرقابل کاهش هستند و باید ریسک را پذیرفت.

۴ جمع بندی و پیشنهادات

در این گزارش مفاهیم کلی هوش تهدید سایبری مورد مطالعه قرار گرفته است و در راستای بهره‌برداری از هوش تهدید سایبری جهت پیشگیری و مقابله با تهدیدات سایبری، دو چارچوب مهم در این زمینه یعنی زنجیره کشتار سایبری و Mitre ATT&CK بررسی گردیده‌اند.

بهره‌برداری از هوش تهدید سایبری و استفاده از چارچوب‌های استاندارد مانند زنجیره کشتار سایبری و MITRE ATT&CK می‌توانند نقشی کلیدی در تقویت امنیت سازمان‌ها ایفا کنند. این چارچوب‌ها با ارائه ساختاری جامع برای شناسایی، تحلیل و پاسخ به تهدیدات سایبری، به سازمان‌ها کمک می‌کنند تا رفتار مهاجمان را بهتر درک کرده و نقاط ضعف خود را با کارایی بیشتری رفع کنند.

استفاده از این چارچوب‌ها جهت بالا بردن توانمندی دفاع سایبری برای سازمان‌ها بسیار ضروری است. با توجه به اینکه چارچوب Mitre ATT&CK مدام در حال بروزرسانی بر اساس تهدیدات جدیدتر و بروزتر و به تبع آن راه‌های مقابله جدیدتر است، استفاده مستمر از آن نقش بسیار مهمی در به‌روزرسانی دانش تیم امنیتی در زمینه تکنیک‌ها و تاکتیک‌های جدید مهاجمان و راه‌های مقابله با آنها دارد.

با توجه به پیچیدگی ذاتی تهدیدات سایبری و مشکل بودن بهره‌برداری کارشناسان امنیتی از پایگاه دانش تهدیدات، استفاده از فناوری‌هایی مثل هوش مصنوعی و یادگیری ماشینی در سامانه‌های هوش تهدید می‌توانند نقش بسیار مهمی در تحلیل خودکار و سریع‌تر اطلاعات امنیتی داشته و اثربخشی شناسایی و پاسخ به تهدیدات را افزایش دهند.

بهره‌برداری از هوش تهدید و استفاده از چارچوب‌های استاندارد، جهت بالا بردن کارایی اشتراک‌گذاری اطلاعات تهدیدات بین سازمان‌ها، به ویژه از طریق مراکز اشتراک‌گذاری اطلاعات مانند ISACها ضروری است. این امر به تحلیل دقیق‌تر تهدیدات و تقویت دفاع جمعی در کشور تاثیر بسزایی دارد و در افزایش تاب‌آوری سایبری سازمان‌ها مؤثر بوده و آمادگی آنها را در برابر تهدیدات نوظهور افزایش می‌دهد.

۵ مراجع

[۱] Guidelines for Applying Threat intelligence in telecommunication network operation, Ttelecommunication Standardization Sector of ITU, ۲۰۲۱.

[۲] Tounsi, W., & Rais, H. (۲۰۱۸). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security, ۷۲, ۲۱۲-۲۳۳.

[۳] Pokorny, Z. (۲۰۱۹). The threat intelligence handbook: Moving toward a security intelligence program. CyberEdge Group: Annapolis, MD, USA.

[۴] X-Force Threat Intelligence Index ۲۰۲۳, IBM Security, ۲۰۲۳.

[۵] Evaluating threat intelligence sources, AO Kaspersky Lab, ۲۰۲۲.

[۶] Martin, L. GAINING THE ADVANTAGE, Applying Cyber Kill Chain Methodology to Network Defense. Lockheed Martin Corporation.

[۷] ۷ Stages of Cyber Kill Chain Supplementary Reading, Deloitte Touche Tohmatsu Limited, ۲۰۱۷.

[۸] Yadav, T., & Rao, A. M. Technical aspects of cyber kill chain. In Security in Computing and Communications: Third International Symposium, SSCC, Kochi, India, August ۱۰-۱۳, ۲۰۱۵. Proceedings ۳ (pp. ۴۳۸-۴۵۲). Springer International Publishing.

[۹] Francesco M. F., Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model: a comparison of cyber intrusion analysis models, ۲۰۲۲.

[۱۰] https://attack.mitre.org/docs/training-cti/CTI Workshop Full Slides.pdf.

[۱۱] Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (۲۰۱۸). Cyber threat intelligence–issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, ۱۰(۱), ۳۷۱-۳۷۹.

[۱۲] Brown, R., & Lee, R. M. (۲۰۱۹). The evolution of cyber threat intelligence (cti): ۲۰۱۹ sans cti survey. SANS Institute. Available online: https://www. sans. org/white-papers/۳۸۷۹۰/(accessed on ۱۲ July ۲۰۲۱).

نشانی: تهران، انتهای کارگر شمالی، پژوهشگاه ارتباطات و فناوری اطلاعات، معاونت پژوهش و توسعه ارتباطات علمی

تلفن: ۰۲۱-۸۸۶۳۰۳۵۵

نمابر: ۰۲۱-۸۸۶۳۰۳۵۶